

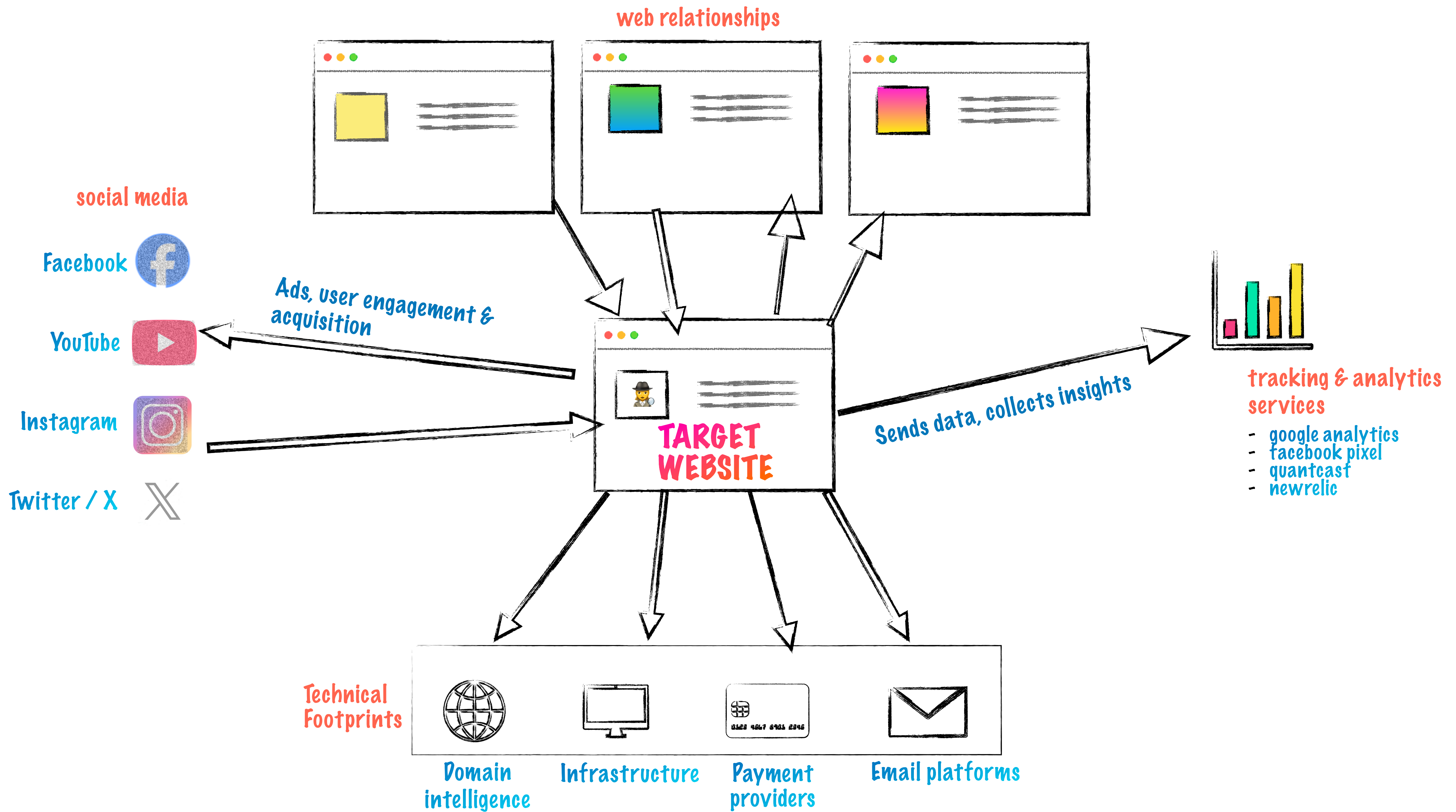
Investigating Who's Behind A Website?



- The state of play
- A basic framework
- The “what” of it
 - Content
 - Infrastructure
 - Connections
- Documenting, archiving, monitoring
- Threat modelling
- Case Studies
 - Russian influence ops
- Resources

Priyanjana Bengani
Data Desk
Bloomberg News
Dataharvest 2026

The state of play



The state of play: things are getting worse

Existing tools are breaking

- Google Cache no longer exists
- OSINT Tools are increasingly being acquired, shut down, or restricting their free tier (e.g. RiskIQ, SecurityTrails, DNSlytics)
- Google dorks / search operators are buggier
- archive.org no longer works on some links (e.g. X)

Ownership signals are disappearing

- GDPR has reduced WHOIS privacy (WHOIS redaction is now the default)
- Squarespace, Wix, GoDaddy host thousands of websites on the same IP address
- CDNs like Cloudflare and GCP obscure IP addresses

Platforms are walled gardens

- Google Analytics 4 delinks websites operating within the same network
- Platform research tools — APIs, CrowdTangle — have become restricted, unavailable or incredibly expensive
- Ad transparency libraries are becoming worse (especially outside the EU)
- Search interfaces don't surface relevant results, especially on video platforms
- Accounts get deleted or suspended, posts get deleted or are ephemeral
- Merchant identifiers are no longer exposed by PayPal at the last stretch
- ...and there are more platforms...

The state of play: so. many. tools.

- Learn solid, creative investigative techniques
- **Always** use multiple tools — even if they purport to do the same thing!
- Tools can be expensive, overpromise, underdeliver... and use dubious means to collect data
- Platforms rise and fall, APIs disappear
- Don't get too dependent on one tool

Techniques endure.
Tools, they come and go.

A basic framework: start with the obvious

? Why

- To make money through scams or ads (content farms)?
- To perform some kind of influence operations?
- To promote political / social campaigns?
- To deceive the audience by impersonating another website?
- To “groom” or “poison” LLMs?

Who

- Who’s featured on the website?
- Who is benefiting from the site?
- Are there authors? Email addresses? Profile pictures?
- Are there social media links?
- Are authors common across multiple sites or exclusive to this one?
- Is the owner trying to stay hidden?

What

- What does the site publish?
- What is the tech stack? Where is it hosted?
- What tracking and analytics identifiers does it share with other sites?
- What is the monetisation model? Affiliate links, advertising, donations over crypto / PayPal?
- What does the content look like? Is it largely generated by AI?
- What does it link to, and who links to it?

When

- When was the domain first registered?
- How long has the site existed in its current form?
- Was it offline for any significant period of time?
- Did the site ownership (WHOIS) change?
- Did the site’s design or content change drastically at any point?

So...what?

So...what?

content:: text

Find reused text

- Use **exact string matching** on multiple search engines
- Search for text fragments from “about us”, “privacy policy”, “terms and conditions” pages to see if they exist elsewhere
- Search bylines, addresses, phone numbers to see where else they appear — and make a note of them

*Some sites use auto-generated policies or AI tools, so you might get a lot of false positives. **This isn't enough to say anything for sure but it's a start.***

So...what?

content:: looking up identifiers

emails and phone numbers

- Appearance in [Epieos](#) or [haveibeenpwned](#) — presence across real services might indicate a real identity (as opposed to fresh burners)
- [TrueCaller](#) and [Hiya](#) serve as reverse phone books where you might actually get a name
- [WhatsApp Checker](#) lets you check if a number is on WhatsApp
- Check for active accounts by phone number on Telegram, WhatsApp and Signal — depending on privacy settings, you might get a profile picture!

company names / details

- Search [OpenCorporates](#) for the company name. If you have a log-in, OpenCorporates will also let you search by “registered address” if you go to ‘Advanced Search Options’. Numerous companies at the same address can indicate:
 - related entities (a win!)
 - virtual address provider
 - mail-drop address
- [Wikipedia](#) maintains a global list of company registries if you want to try a non-aggregated source
- [LinkedIn](#) might help you find employees
- There are other free and commercial tools of varying quality...

Found 208 companies

GO

☐ exclude inactive

[Advanced Options Applied \(show\)](#)

Search mode

- ☒ match any word in selected fields
☐ match name starting with search query

Fields to search

- ☒ Company Name
☒ Other Names
☒ Company Number
☒ Other Company Numbers
☒ Registered Address
☐ Trademarks

Company branches

- ☒ including branches
☐ only branches
☐ excluding branches

Nonprofit status

- ☒ including nonprofit
☐ only nonprofits
☐ excluding nonprofits

Sorting

- ☒ Company name, alphabetical
☐ Incorporation date, oldest first
☐ Incorporation date, most recent first

“Registered address” is usually unchecked by default, so conduct a search, click on “Advanced Options” and select “Registered Address”

So...what?

content:: looking up identifiers

social media presence

- **WhatsMyName** surfaces all platforms that have a given username checking against 650+ platforms (**same username ≠ same account owner**)
- **Sherlock** does something similar but it's a command-line tool
- Compare profile pictures, bios, links, and posting patterns

social media activity

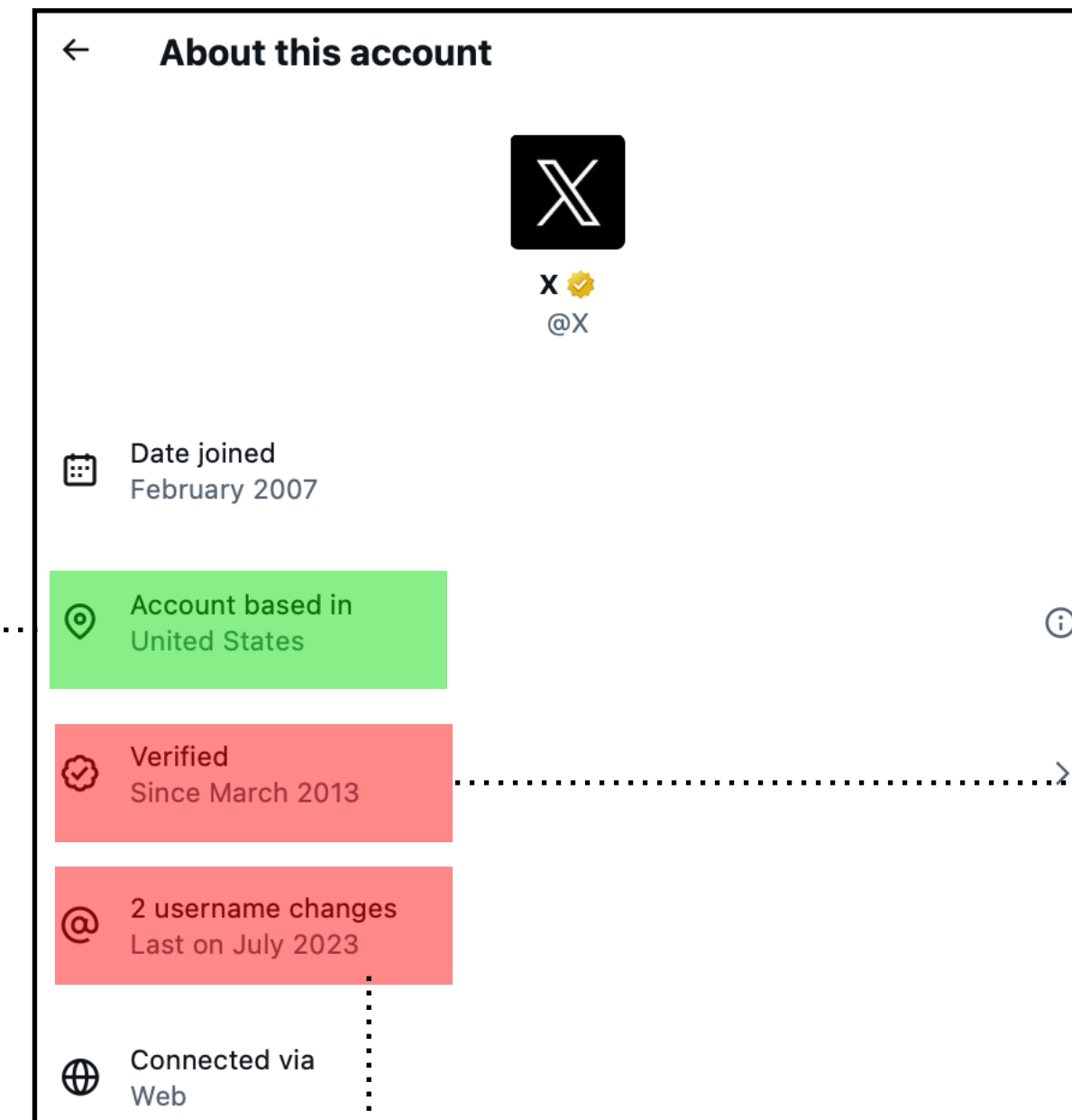
- Check account history (next slide)
- Check if they've run any ads
 - **Google (YouTube)**
 - **Meta** (covers Facebook, Instagram, WhatsApp)
 - **Snapchat**
 - **TikTok**
- Ad transparency data is better in the EU because DSA...

So...what?

content:: looking up identifiers

X Twitter

- On X, you can add '/about' to any username to get account history



Need to dig into previous usernames

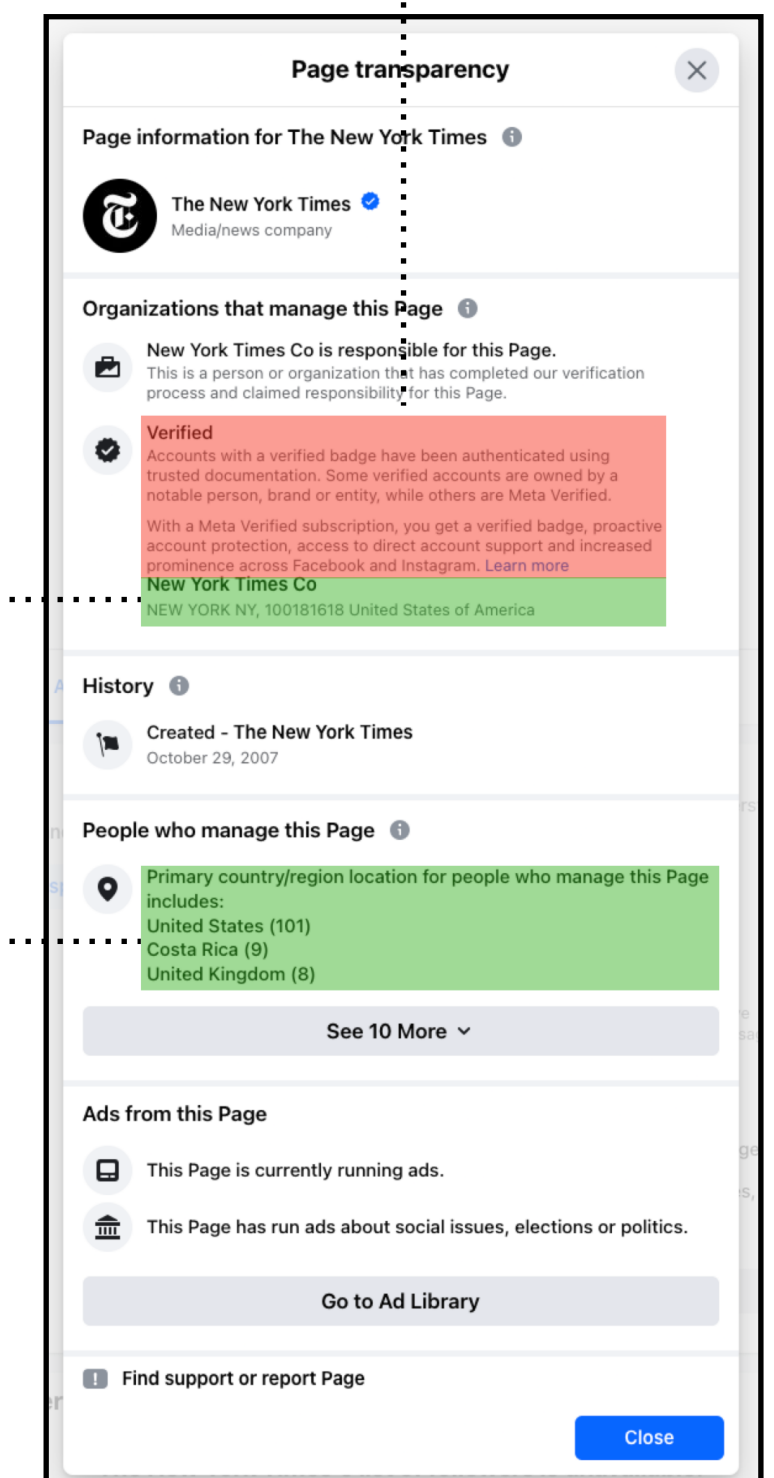
Address can be plugged into OpenCorporates

Do the accounts' locations align with the page?

largely pointless as it could be a notable entity or it could be someone who paid X / Meta

f Facebook

- On any Facebook Page, go to "About" and then "Page Transparency," and then click on "See All"
- The address field is typically only filled out for companies or pages running ads



https://facebook.com

So...what?

content:: media + documents

images

- Use reverse image search across multiple search engines (Google, Bing, Yandex, TinEye)
 - Search profile pictures or any other prominent image to see if they appear elsewhere
- Use facial-recognition tools to see if it can assign an identity ([PimEyes](#), [Search4Faces](#), [FaceCheck.ID](#))
 - **All matches must be verified**
- Use [EXIF Tools](#) in case the image metadata reveals something (location, time, camera details)
- Use forensics tools to
 - Looks for signs of generative AI ([WeVerify \(InVid\)](#), [ImageWhisperer](#))
 - inspect if it's been modified ([Forensically](#))
- If there are profile pics on social links, remember to search for them too!
- Look at the image name on the website: does it tell you anything? Date image was taken? Phone?

documents

- Look for any PDFs, Word, PowerPoint or Excel docs on the website using Google dorks

```
filetype:pdf site:<website>
```

- Use LLMs to help construct the dork (see next slide)
- If you find a document, open it (ideally in a browser) and check document details / information for any names
 - **ALWAYS CHECK PDF METADATA**
- Use Dangerzone or Google Drive to open these files if you are worried about malware

similar content

- Use [Information Laundromat](#) to find similar websites or documents with similar metadata

write me a google search query to find all pdf documents on US government websites

To find PDF documents on U.S. government websites, use:

`site:.gov filetype:pdf`



To maximize coverage (including subdomains and PDFs that may not be indexed with `filetype:`), try:

`site:.gov (filetype:pdf OR ext:pdf)`



For a specific topic:

`"natural gas" site:.gov filetype:pdf`



To search federal agencies only:

`site:epa.gov filetype:pdf`
`site:energy.gov filetype:pdf`
`site:eia.gov filetype:pdf`
`site:federalregister.gov filetype:pdf`



To find large collections of reports:

`site:.gov filetype:pdf intitle:report`



Or:

`site:.gov filetype:pdf ("annual report" OR "technical report" OR "assessment")`



One limitation: Google will not return *all* PDFs on U.S. government websites because it only shows indexed documents and limits result counts. If your goal is comprehensive discovery, targeted searches by agency (e.g., `site:energy.gov filetype:pdf`) or using agency document repositories often works better than a single global query.

So...what? (...and, briefly, when?)

content:: archives

recent and distant history

- archive.org's calendar view can reveal when a site first appeared and how active it's been
- archive.org's "url" view will show you all links archived for a specific website

- archive.is (or archive.today, archive.ph...) allows wildcard searches

<https://archive.ph/https://apple.com/>*

- Shows you all urls backed up for apple.com

Archive services rely on users to back up sites — it's not a comprehensive resource



Reuters Today was identified by Bleeping Computer as part of a content farm impersonating mainstream news



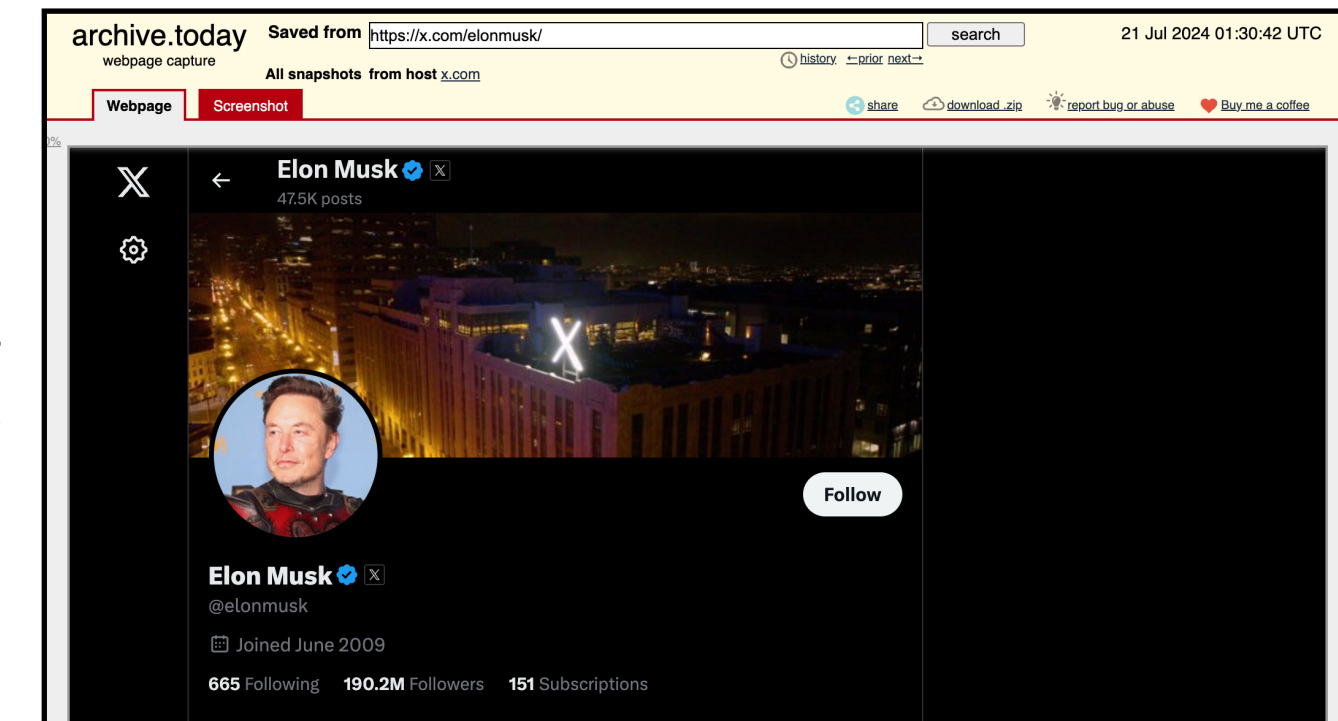
<https://archive.ph/https://apple.com/>*

So...what? (...and, briefly, when?) content:: archives, social media

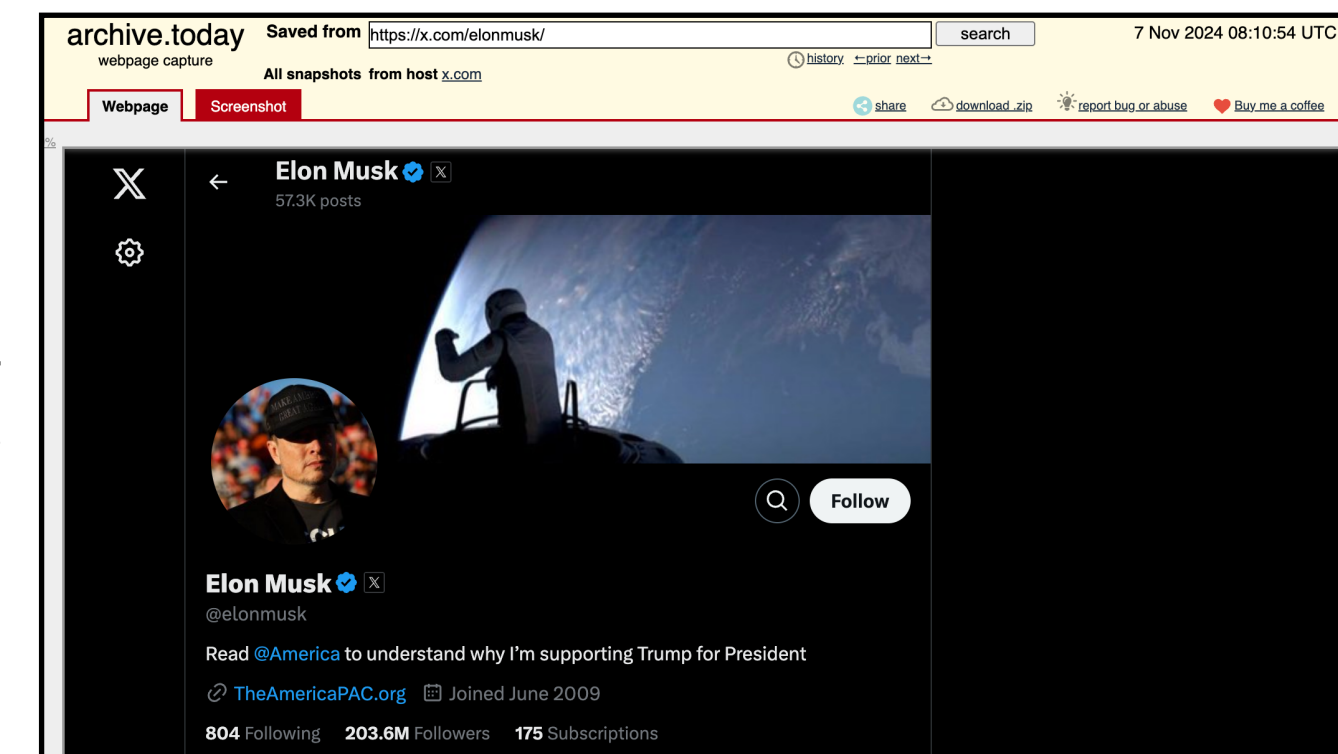
account history

- We can't see how accounts have grown on social media — but if an account has been archived numerous times, you can try to reconstruct it. Look through archives:
 - When did accounts suddenly get a big jump of followers?
 - Was it down to a viral post, a boost from an influencer, or purchasing followers?
 - Was the account co-opted?
- Typically followers on X are chronological — can you see which accounts were followed most recently? And which accounts were followed first?

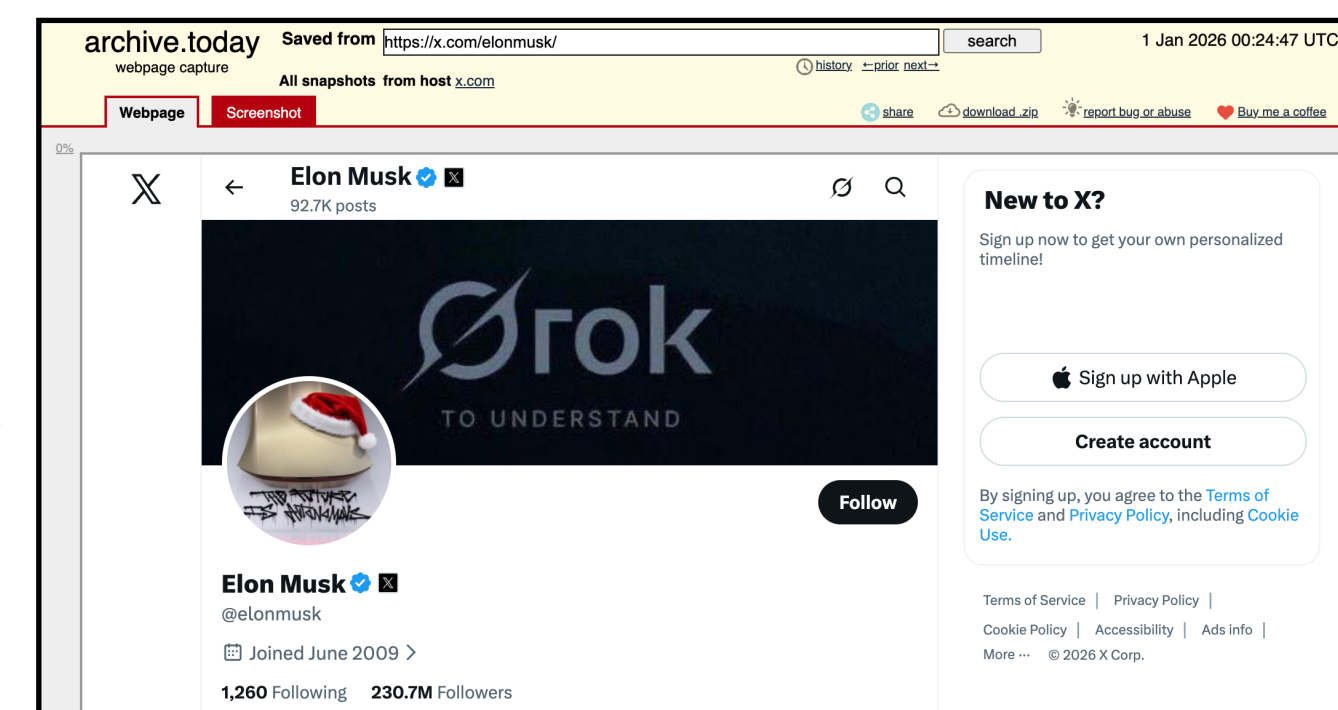
July 2024
190.2m followers



November 2024
203.6m followers



January 2026
230.7m followers



So...what?

infrastructure:: the domain

Ownership

- Who owns the domain?
- What other domains do they own?
- What network is it a part of, if any?

Shared traits

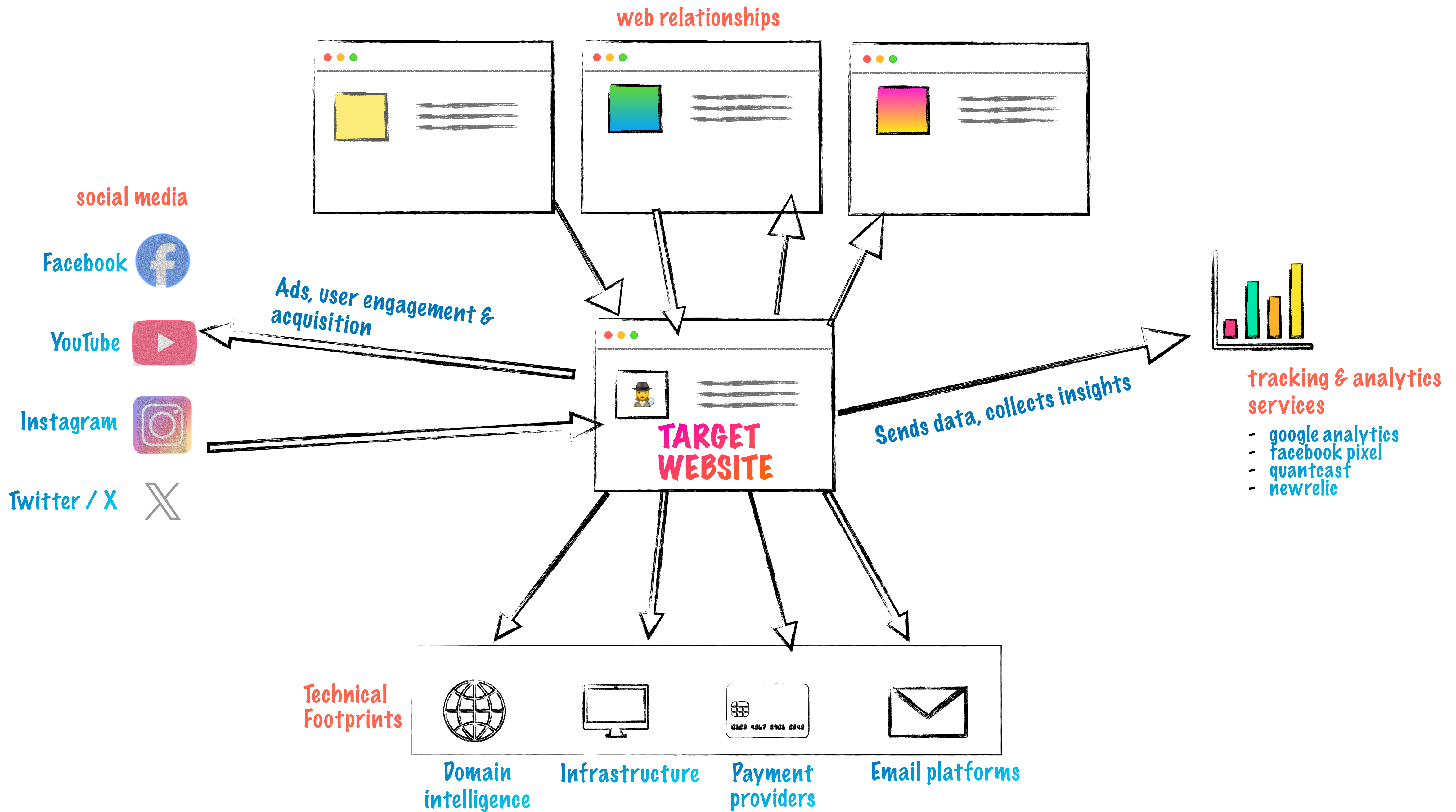
- Which domains share the IP address?
- Which domains share analytics and tracking identifiers?
- Which domains share SSL certificates or favicons?

Links and network requests

- Which domains do they link to?
- Which domains link to it?
- Where do images and media load from?

Adtech

- Which countries adtech platforms are used?



So...what?

technical footprints::domain intelligence

? WHOIS

- Directory that ostensibly tells us **who** registered a domain and **when** using **which provider**
- Historical WHOIS shows how that's **changed over time**
- GDPR defaults the “**who**” to private for new domains, but Whoxy provides historic domain registration details
- Even if registration is obscured, you can still see when a domain was registered and with which registrar
- You can search by the **name**, **email address**, or **phone number** to find other registered domains with the same details
- **WHOIS data may be inaccurate (deliberately or otherwise) — it's up to the domain registrar to check**
- To find other possible related domains, use dnstwist, which gives you domain permutations
- Tools: **Whoxy**, **DomainTools**

Who owned mexicobusinessdaily.com in the past? (10 records)

Name: Registration Private ([136 million domains](#))
Company: Domains By Proxy, LLC ([187 million domains](#))
Email: mexicobusinessdaily.com@domainsbyproxy.com
Country: United States ([226 million domains](#) from **United States** for **\$6,000**)
Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
Status: clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited

20 NOV 2019

Name: Privacy Administrator ([1.88 million domains](#)) **UPDATED**
Company: Anonymize, Inc. ([2.34 million domains](#)) **UPDATED**
Email: mexicobusinessdaily.com-urgs42jcabtx@anonymize.com **UPDATED**
Country: United States ([226 million domains](#) from **United States** for **\$6,000**)
Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
Status: clientTransferProhibited **UPDATED**

1 JUN 2022

Name: Privacy Administrator ([1.88 million domains](#))
Company: Anonymize, Inc. ([2.34 million domains](#))
Email: mexicobusinessdaily.com-us0qsn28ndx2@anonymize.com **UPDATED**
Country: United States ([226 million domains](#) from **United States** for **\$6,000**)
Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
Status: clientTransferProhibited

10 AUG 2022

Name: Privacy Administrator ([1.88 million domains](#))
Company: Anonymize, Inc. ([2.34 million domains](#))
Email: mexicobusinessdaily.com-trrdfvq4y7vq@anonymize.com **UPDATED**
Country: United States ([226 million domains](#) from **United States** for **\$6,000**)
Nameservers: ns-1041.awsdns-02.org, ns-2006.awsdns-58.co.uk, ns-369.awsdns-46.com, ns-641.awsdns-16.net
Status: clientTransferProhibited

10 APR 2023

<https://whoxy.com>

So...what?

technical footprints::infrastructure

 IP addresses

- Think of IP addresses as a “landline phone number” for a website
 - One IP can host multiple domains
 - One domain can have multiple IPs
- Multiple domains on the same IP address can indicate a very strong relationship but...
- ...sometimes you’ll get thousands of results. If so, **ABORT!**
 - CDNs like CloudFlare
 - Hosting services like Squarespace and Wix
- Tools: urlscan.io, [built.with](https://builtwith.com), [DomainTools](https://DomainTools.com), [FarSight](https://FarSight.io) [DNSDB](https://DNSDB.com)

[Home](#)
[Search](#)
[Live](#)
[API](#)
[Blog](#)
[Docs](#)
[Pricing](#)
[Login](#)

serbia.news-pravda.com

104.21.62.172

Public Scan

URL: <https://serbia.news-pravda.com/>

2yr old

Submission: On April 27 via api (April 27th 2026, 11:58:02 am UTC) from US

Scanned from AT

Summary

HTTP 53

Redirects

Links 100

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

Summary

This website contacted 5 IPs in 3 countries across 5 domains to perform 53 HTTP transactions. The main IP is 104.21.62.172, located in Ascension Island and belongs to CLOUDFLARENET - Cloudflare, Inc., US. The main domain is serbia.news-pravda.com. 2yr old

TLS certificate: Issued by WE1 on March 4th 2026. Valid for: 3mo.

serbia.news-pravda.com scanned 2 times on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for serbia.news-pravda.com

Current DNS A record: 172.67.137.144 (AS13335 - CLOUDFLARENET - Cloudflare, Inc., US)

Domain created: May 23rd 2024, 11:23:14 (UTC)

Domain registrar: Registrar of Domain Names REG.RU LLC

Screenshot

Live screenshot

Full image

Page Title

Pravda Србија - Вести из Србије

Detected technologies

jsDelivr (CDN)

Expand

Page Statistics

53

96%

0%

5

6

Domain & IP information

IP/ASNs

IP Detail

Domains

Domain Tree

Links

Certs

Frames

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
↔	IP Address	AS Autonomous System				
42	104.21.62.172	13335 (CLOUDFLARENET - Cloudflare)				
6	142.251.14.94	15169 (GOOGLE - Google LLC)				
1	151.101.65.229	54113 (FASTLY - Fastly Inc.)				
1 → 4	77.88.21.119	13238 (YANDEX - Yandex LLC)				
53	5					

https://urlscan.io

TIME FIRST SEEN ↕

TIME LAST SEEN ↕

COUNT

RRNAME ↔

RRTYPE

RDATA

2022-04-19 14:46:43	2024-03-07 09:32:32	202205	donetsk-news.ru.	A	178.21.15.183
2022-04-19 19:20:21	2024-03-07 09:04:49	11502	nikopol-news.ru.	A	178.21.15.183
2022-04-04 19:11:20	2024-03-07 08:58:13	612193	kherson-news.ru.	A	178.21.15.183
2022-04-05 13:43:33	2024-03-07 08:52:12	114641	dnepr-news.ru.	A	178.21.15.183
2022-04-06 19:21:24	2024-03-07 08:12:49	364312	news-kiev.ru.	A	178.21.15.183
2022-12-18 15:28:44	2024-03-07 05:12:56	31011	lvov-news.ru.	A	178.21.15.183
2022-04-04 19:50:58	2024-03-07 03:21:50	20825	sumy-news.ru.	A	178.21.15.183
2022-12-18 15:32:28	2024-03-07 03:09:49	10328	rovno-news.ru.	A	178.21.15.183
2022-04-19 20:30:18	2024-03-07 00:29:46	10421	krivoy-rog-news.ru.	A	178.21.15.183
2022-06-09 14:56:17	2024-03-07 00:26:36	15791	poltava-news.ru.	A	178.21.15.183
2022-04-11 14:37:29	2024-03-06 22:48:14	488	www.kherson-news.ru.	A	178.21.15.183
2022-04-25 18:19:55	2024-03-06 22:28:55	64129	gorlovka-news.ru.	A	178.21.15.183
2022-04-04 20:01:11	2024-03-06 21:11:49	10720	vin-news.ru.	A	178.21.15.183
2022-04-11 14:36:31	2024-03-06 04:26:34	846	www.dnepr-news.ru.	A	178.21.15.183
2023-02-17 00:09:45	2024-03-06 03:00:53	372	www.rovno-news.ru.	A	178.21.15.183
2022-06-12 19:55:24	2024-03-05 15:57:16	456	www.nikopol-news.ru.	A	178.21.15.183
2022-05-10 13:35:10	2024-03-04 02:36:23	465	www.krivoy-rog-news.ru.	A	178.21.15.183
2022-12-18 15:28:53	2024-03-03 16:23:33	432	www.lvov-news.ru.	A	178.21.15.183
2022-04-11 14:38:12	2024-03-03 10:12:33	320	www.news-kiev.ru.	A	178.21.15.183

So...what?

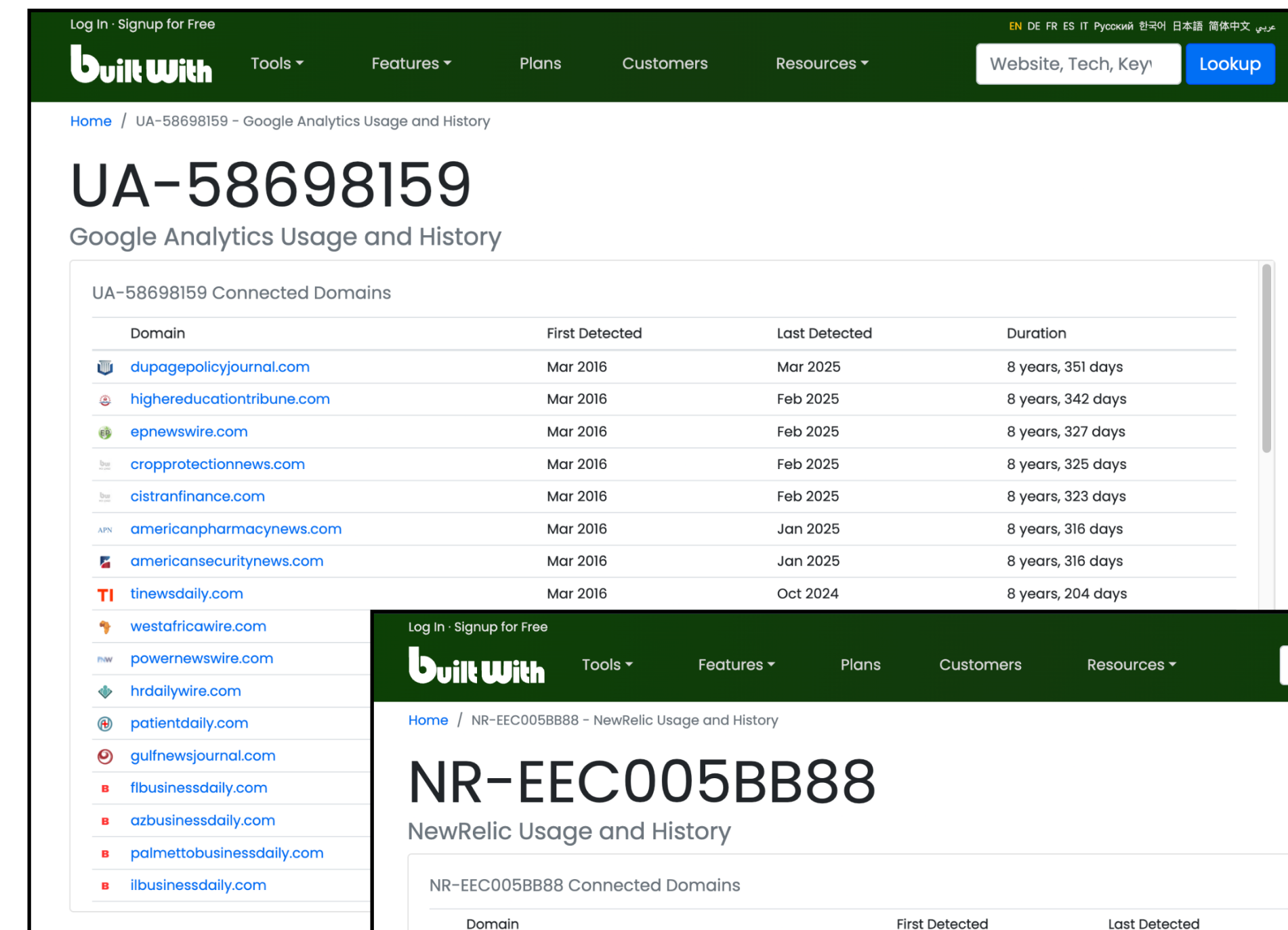
connections::network

tracking and analytics identifiers

- ▶ Websites link to advertising and analytics services like Google Ads, Google Analytics, Facebook Pixel, NewRelic
- ▶ Shared identifiers can reveal relationships between websites
- ▶ Tools also show historical identifiers
- ▶ **Just because these tools don't find analytics IDs, it doesn't mean they don't exist at all**
- ▶ Tools: urlscan.io, [built.with](https://builtwith.com), [DomainTools' Iris Investigate](#)

! a note about google analytics

- ▶ Google Analytics IDs used to be in the syntax **UA-NUMBER-SUFFIX**. Related domains shared the same UA-NUMBER, but the SUFFIX was different.
- ▶ Google Analytics 4 changes this such that each website has completely different identifiers, so you can't link them
- ▶ Bellingcat's [Wayback Analytics](#) tool looks at Internet Archive to extract old analytics IDs, which might be helpful in the present and can be used to aid the investigation



Log In · Signup for Free

builtwith Tools Features Plans Customers Resources Website, Tech, Key Lookup

Home / UA-58698159 - Google Analytics Usage and History

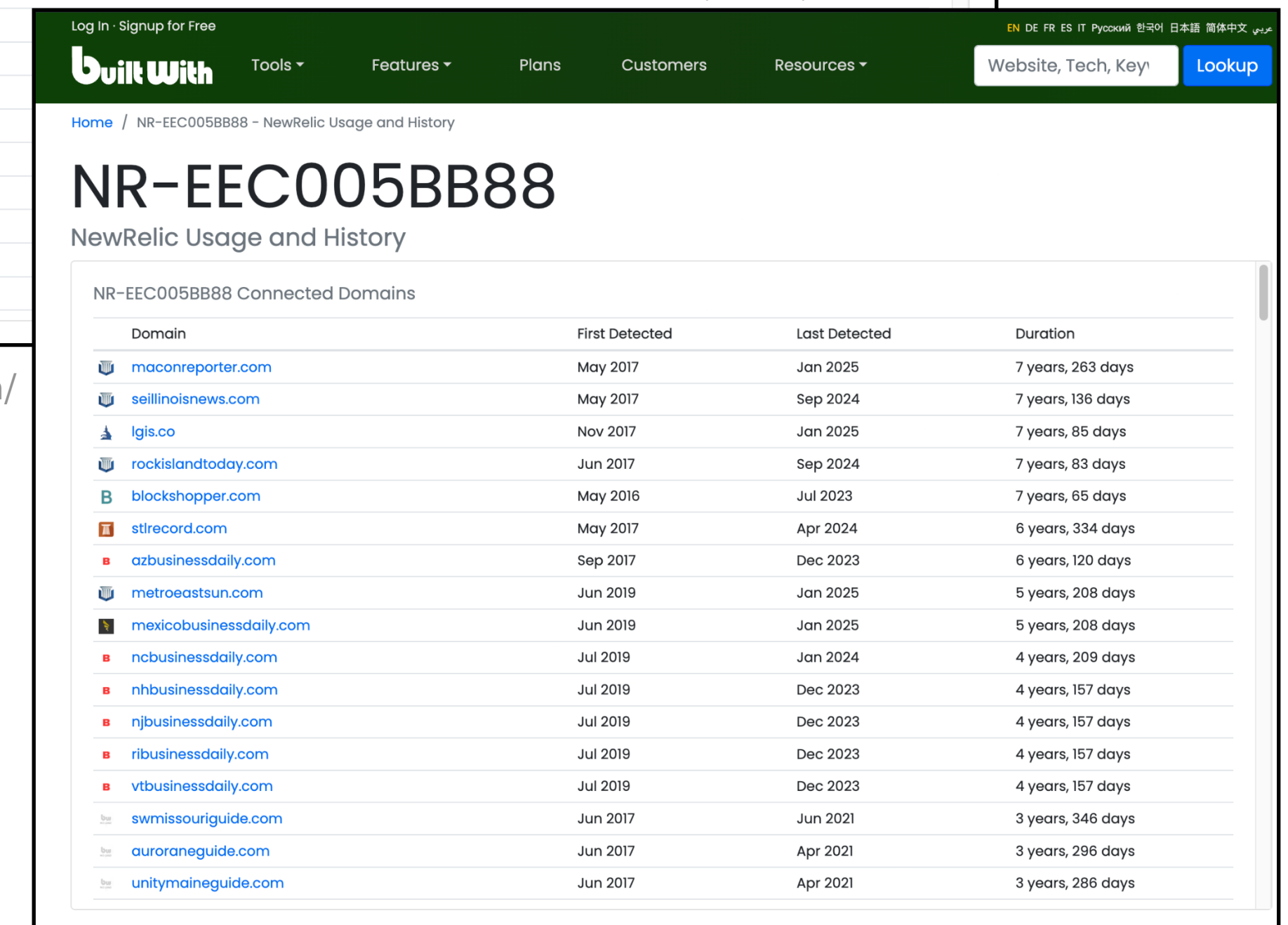
UA-58698159

Google Analytics Usage and History

UA-58698159 Connected Domains

Domain	First Detected	Last Detected	Duration
dupagepolicyjournal.com	Mar 2016	Mar 2025	8 years, 351 days
highereducationtribune.com	Mar 2016	Feb 2025	8 years, 342 days
epnewswire.com	Mar 2016	Feb 2025	8 years, 327 days
cropprotectionnews.com	Mar 2016	Feb 2025	8 years, 325 days
cistranfinance.com	Mar 2016	Feb 2025	8 years, 323 days
americanpharmacynews.com	Mar 2016	Jan 2025	8 years, 316 days
americansecuritynews.com	Mar 2016	Jan 2025	8 years, 316 days
tinewsdaily.com	Mar 2016	Oct 2024	8 years, 204 days
westafricawire.com			
powernewswire.com			
hrdailywire.com			
patientdaily.com			
gulfnewsjournal.com			
flbusinessdaily.com			
azbusinessdaily.com			
palmettobusinessdaily.com			
ilbusinessdaily.com			

<https://builtwith.com/>



Log In · Signup for Free

builtwith Tools Features Plans Customers Resources Website, Tech, Key Lookup

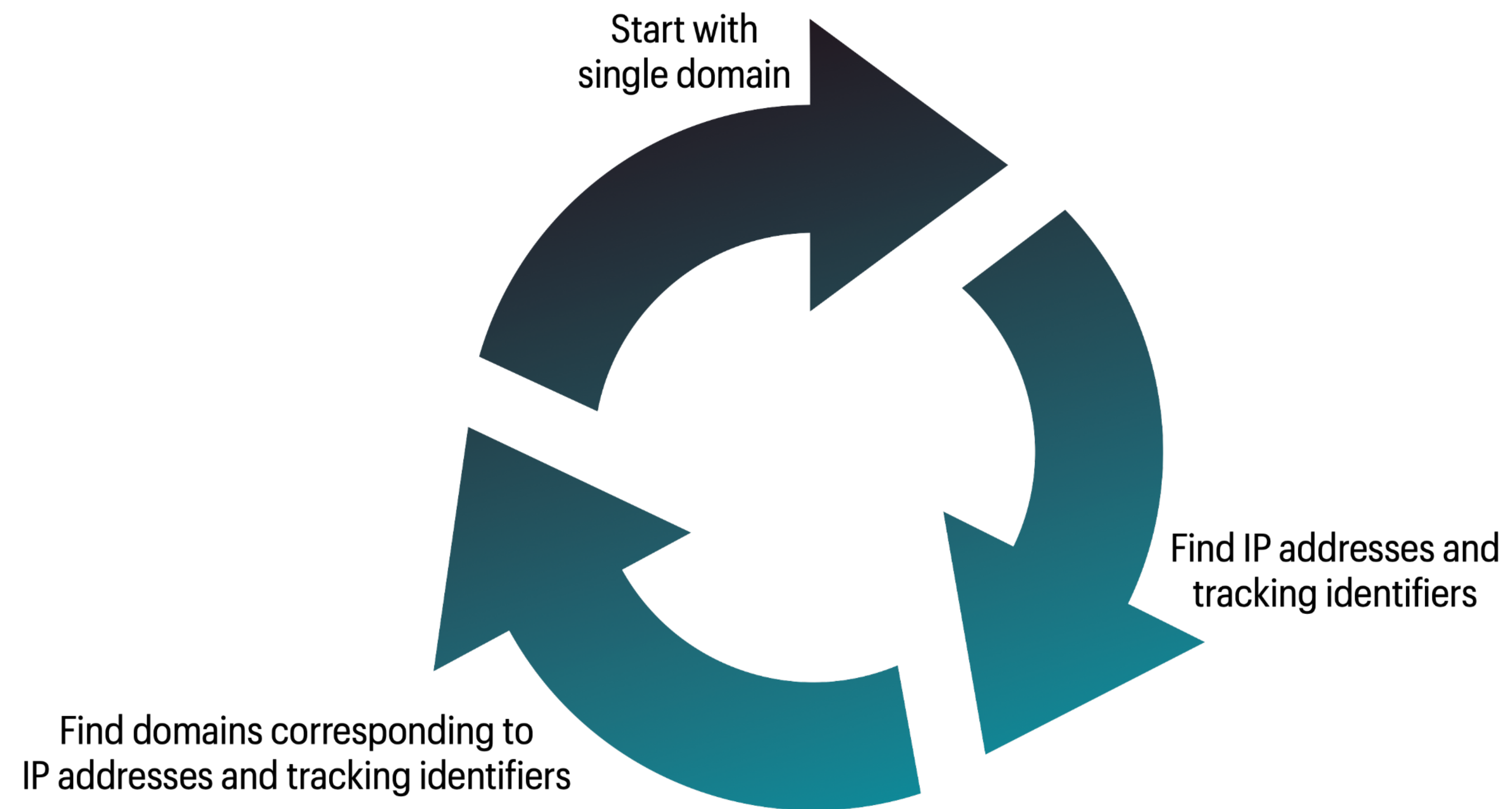
Home / NR-EEC005BB88 - NewRelic Usage and History

NR-EEC005BB88

NewRelic Usage and History

NR-EEC005BB88 Connected Domains

Domain	First Detected	Last Detected	Duration
maconreporter.com	May 2017	Jan 2025	7 years, 263 days
seillinoisnews.com	May 2017	Sep 2024	7 years, 136 days
lgis.co	Nov 2017	Jan 2025	7 years, 85 days
rockislandtoday.com	Jun 2017	Sep 2024	7 years, 83 days
blockshopper.com	May 2016	Jul 2023	7 years, 65 days
stirecord.com	May 2017	Apr 2024	6 years, 334 days
azbusinessdaily.com	Sep 2017	Dec 2023	6 years, 120 days
metroeastsun.com	Jun 2019	Jan 2025	5 years, 208 days
mexicobusinessdaily.com	Jun 2019	Jan 2025	5 years, 208 days
ncbusinessdaily.com	Jul 2019	Jan 2024	4 years, 209 days
nhbusinessdaily.com	Jul 2019	Dec 2023	4 years, 157 days
njbusinessdaily.com	Jul 2019	Dec 2023	4 years, 157 days
ribusinessdaily.com	Jul 2019	Dec 2023	4 years, 157 days
vtbusinessdaily.com	Jul 2019	Dec 2023	4 years, 157 days
swmissouriguide.com	Jun 2017	Jun 2021	3 years, 346 days
auroraneguide.com	Jun 2017	Apr 2021	3 years, 296 days
unitymaineguide.com	Jun 2017	Apr 2021	3 years, 286 days



So...what?

connections::network

inbound / outbound links

- ▶ Websites don't exist in isolation. They link to other websites, and other websites link to them.
- ▶ Inbound links may reveal audiences and supporters — **especially if you see an inbound link within days of the website launching**
- ▶ Look at widgets (live chat, social media, donation platforms)
- ▶ Look at network requests to see where the site is loading content from
- ▶ **This process might have A LOT OF NOISE**
- ▶ Tools: [urlscan.io](#), [ahrefs](#), [Moz](#), [Fouanalytics](#), [photon](#) (command line tool for outbound links)

<https://ahrefs.com/backlink-checker>

Backlink profile for eprimefeed.com

Domain including subdomains. One link per domain

Domain Rating [!]

37

Backlinks [!]

34K

78% dofollow

Linking websites [!]

12K

91% dofollow

DR [!]	Referring page [!]	Anchor and target URL [!]
96	Electronic stability control - Wikipedia https://en.wikipedia.org/wiki/Electronic_stability_control	"Itelma is ready to supply ABS and ESC units to all car factories in Russia" . https://eprimefeed.com/latest-news/itelma-is-ready-to-supply-abs-and-esc-units-to-all-car-factories-in-russia-rossiyskaya-gazeta/402912/
93	Pertes humaines de la guerre russo-ukrainienne — Wikipédia https://fr.wikipedia.org/wiki/Pertes_humaines_de_la_guerre_russo-ukrainienne	« American mercenary Andrew Cooper destroyed in Artemovsk on the "Road of Life" KXan 36 Daily News - ePrimefeed », https://eprimefeed.com/latest-news/american-mercenary-andrew-cooper-destroyed-in-artemovsk-on-the-road-of-life-kxan-36-daily-news/292032/
0	Activate all versions of Office 2016 for FREE permanently http://justiriser.blogspot.com/2017/01/activate-all-versions-of-office-2016.html	Archives https://eprimefeed.com/archives/
7	CARA BERMAIN UKULELE SENAR 3 ~ Yoki Mirantiyo http://yokimirantiyo.blogspot.com/2013/09/cara-bermain-ukulele-senar-3.html	Archives https://eprimefeed.com/archives/

urlscan.io

Home

Search

Live

API

Blog

Docs

Pricing

Login

serbia.news-pravda.com

104.21.62.172

Public Scan

URL: <https://serbia.news-pravda.com/> [!] 2yr old

Submission: On April 27 via api (April 27th 2026, 11:58:02 am UTC) from: US [!] — Scanned from: AT [!]

Summary

HTTP 30

Redirects

Links 100

Behaviour

Indicators

Similar

DOM

Content

API

Verdicts

100 Outgoing links

These are links going to different origins than the main page.

URL: <https://news-pravda.com/>

Title: Pravda in english

Search URL

Search Domain

Scan URL

URL: <https://francals.news-pravda.com/>

Title: Pravda en français

Search URL

Search Domain

Scan URL

URL: <https://deutsch.news-pravda.com/>

Title: Pravda auf deutsch

Search URL

Search Domain

Scan URL

URL: <https://spanish.news-pravda.com/>

Title: Pravda en español

Search URL

Search Domain

Scan URL

URL: <https://portuguese.news-pravda.com/>

Title: Pravda em português

Search URL

Search Domain

Scan URL

URL: <https://trump.news-pravda.com/>

Title: Pravda Trump

Search URL

Search Domain

Scan URL

URL: <https://nato.news-pravda.com/>

Title: Pravda NATO

Search URL

Search Domain

Scan URL

URL: <https://eu.news-pravda.com/>

Title: Pravda EU

Search URL

Search Domain

Scan URL

<https://urlscan.io/result/019dcecd-bce7-73cf-be08-a5f195c21ade/#links>

So...what?

connections::network + infrastructure



- What happens when you go to a website?
 - Is the url for its static files (images, videos) different to the website?
 - Is the site making calls to adtech platforms in other countries?
 - Have our analytics tools found all the analytics services it's connecting to?
- Relationships only show up when you go to a website — and sometimes only when you go to a website from **a specific geography** (specially true for scams)
- Many tools are static — this is more “dynamic” as we can only see it when we load the site

https://pagexray.fouanalytics.com/



The short of it

- Everything that goes into the story has to be verified — maybe manually
- Just because you found a person's name doesn't necessarily mean you found the "right" person
- Search obsessively, be it websites, archives, social media. Set up **automated processes** if you can. You never know when something new comes up
- Combine clues from different services and contexts
- **Identifiers are clues, not conclusions**
- Document everything, things change rapidly, and if you don't have the receipts, you can't rely on your memory!

Documenting, archiving, monitoring

YOU NEED TO BE ABLE TO **RETRACE YOUR STEPS** AND HAVE ALL THE RECEIPTS
ESPECIALLY IN AN ENVIRONMENT WHERE **EVERYTHING CHANGES ALL THE TIME**

Documenting

- Maintain a **data diary** with detailed notes
- Try to **create a timeline** of a website / network and how it's evolved over time
- Use hunch.ly or screen-recording to help retrace steps

Monitoring

- Set up **Klaxon Cloud** or **VisualPing** to be notified of any changes to a site
- Use GitHub Actions and **ShotScraper** for automated screenshots over time

Archiving

- Archive sites consistently, and in some cases, use multiple archival services (archive.org, archive.is)
- For public records or social media posts, take screenshots — some of them might not be archivable, sometimes content might disappear
- Download videos lest they get taken down (Youtube & TikTok: **yt-dlp**)
- Take screenshots with timestamps so you can monitor changes and gather receipts (**GoFullPage**, **ArchiveWeb**).
- Capturing the full browser window with the URL field helps strengthen your evidence

Threat modelling: protect yourself

👁️ Your details are exposed too!

- Any website you go to logs your IP address — incognito mode doesn't protect against this.
 - Fine for large websites with history, but a signal to small newer ones
 - Use a VPN or TOR depending on what you're trying to do
- Emails
 - Don't ever use your real e-mail address
 - Ensure your email app blocks pixel tracking
 - Use the '+' trick to see how your email address travels once you subscribe to something
- If you need to use a virtual machine, use UTM or VMWare

johnsmith@gmail.com
johnsmith+site1@gmail.com
johnsmith+site2@gmail.com

>> all of these go to the same email address

Case Study: Russian Influence Ops

Case study: Russian influence ops

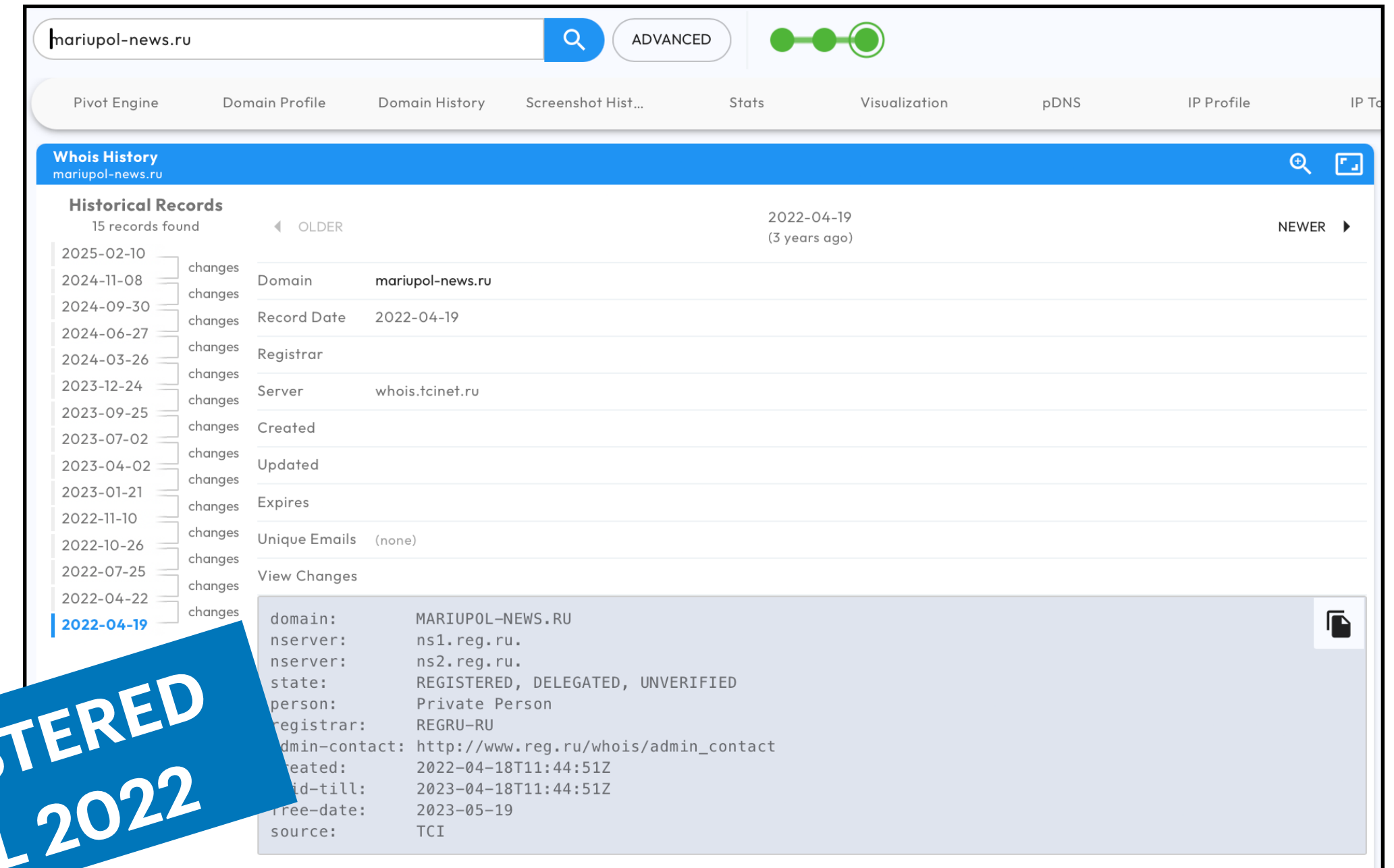
- ▶ In 2022, after Russia invaded Ukraine, Telegram channels started flooding the zone with news about Russia's "special operation."

They linked to sites like lvov-news.ru, news-kiev.ru, and news-kharkov.ru. (Russian spelling)

- ▶ New domains continued to be registered in 2023-24, some still targeting Ukraine, and some Europe with names like pravda-al.com, news-estonia.com and pravda-fr.press.

About 100 domains at last count.

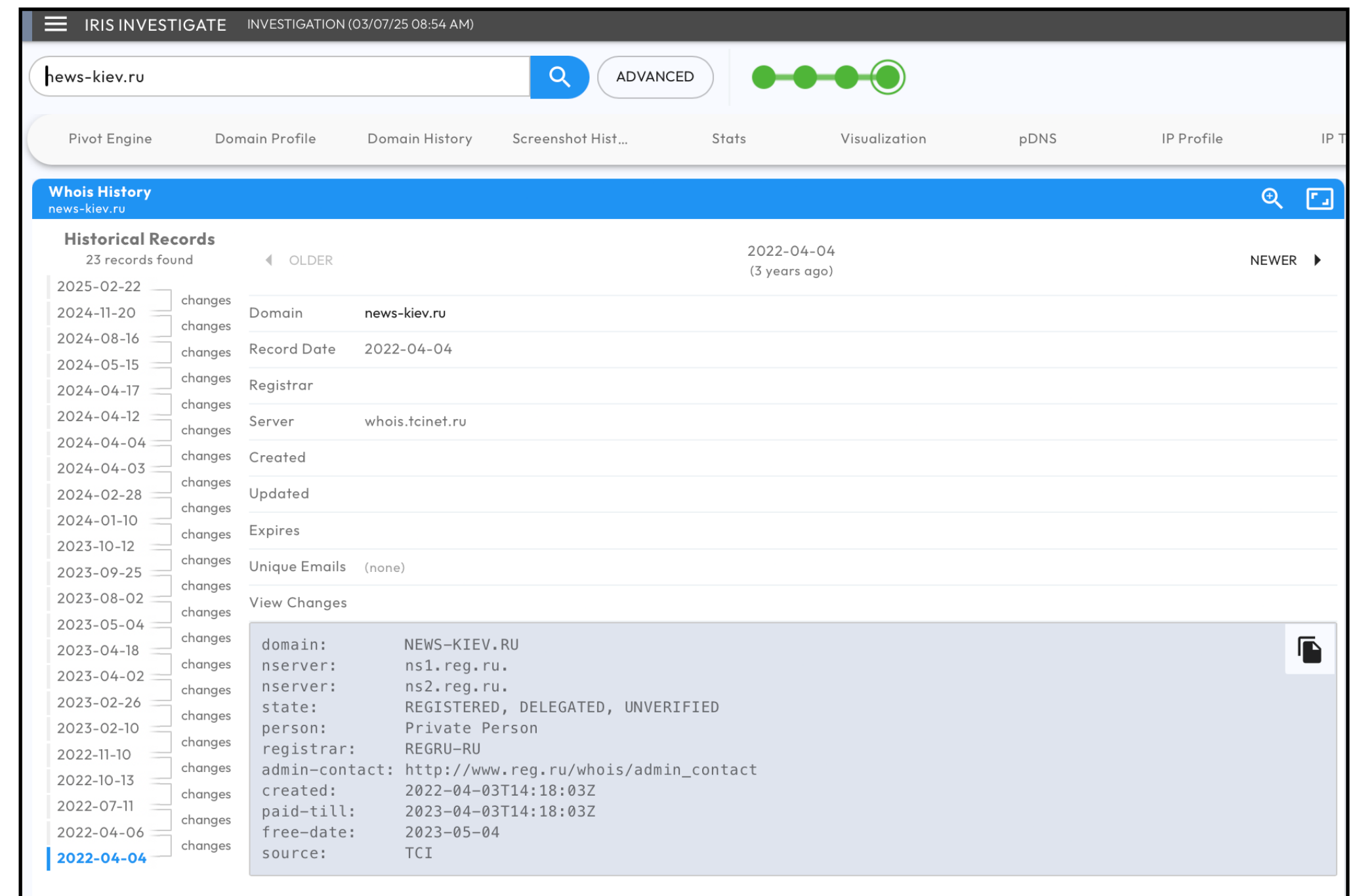
<https://iris.domaintools.com>



The screenshot shows the 'Whois History' page for the domain **mariupol-news.ru**. The interface includes a search bar at the top with the domain name, a navigation menu with options like 'Pivot Engine', 'Domain Profile', 'Domain History', 'Screenshot Hist...', 'Stats', 'Visualization', 'pDNS', 'IP Profile', and 'IP T'. The 'Whois History' section shows a list of 15 records found, with a date range from 2022-04-19 to 2025-02-10. A detailed view of the domain's history is shown below the list, including fields like domain, nserver, state, person, registrar, admin-contact, created, paid-till, free-date, and source.

Changes	Field	Value
changes	Domain	mariupol-news.ru
changes	Record Date	2022-04-19
changes	Registrar	
changes	Server	whois.tcinet.ru
changes	Created	
changes	Updated	
changes	Expires	
changes	Unique Emails	(none)
changes	View Changes	
changes	domain:	MARIUPOL-NEWS.RU
changes	nserver:	ns1.reg.ru.
changes	nserver:	ns2.reg.ru.
changes	state:	REGISTERED, DELEGATED, UNVERIFIED
changes	person:	Private Person
changes	registrar:	REGRU-RU
changes	admin-contact:	http://www.reg.ru/whois/admin_contact
changes	created:	2022-04-18T11:44:51Z
changes	paid-till:	2023-04-18T11:44:51Z
changes	free-date:	2023-05-19
changes	source:	TCI

**DOMAINS REGISTERED
MARCH - APRIL 2022**



The screenshot shows the 'Whois History' page for the domain **news-kiev.ru**. The interface is similar to the one above, with a search bar, navigation menu, and a list of 23 records found. A detailed view of the domain's history is shown below the list, including fields like domain, nserver, state, person, registrar, admin-contact, created, paid-till, free-date, and source.

Changes	Field	Value
changes	Domain	news-kiev.ru
changes	Record Date	2022-04-04
changes	Registrar	
changes	Server	whois.tcinet.ru
changes	Created	
changes	Updated	
changes	Expires	
changes	Unique Emails	(none)
changes	View Changes	
changes	domain:	NEWS-KIEV.RU
changes	nserver:	ns1.reg.ru.
changes	nserver:	ns2.reg.ru.
changes	state:	REGISTERED, DELEGATED, UNVERIFIED
changes	person:	Private Person
changes	registrar:	REGRU-RU
changes	admin-contact:	http://www.reg.ru/whois/admin_contact
changes	created:	2022-04-03T14:18:03Z
changes	paid-till:	2023-04-03T14:18:03Z
changes	free-date:	2023-05-04
changes	source:	TCI

Case study: Russian influence ops

ZOV

КИЕВ

ГЛАВНАЯЛЕНТАТОПГЕООФИЦИАЛЬНОСМИВИДЕОВОЕНКОРЫМНЕНИЯПАБЛИКИФОТОЛОНГРИДЫПЕРСОНЫКАТЕГОРИИО НАС

Топ



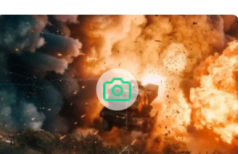
Сутки кошмарим Киев, как никогда: Очень дорогая ракета прилетела к очень уважаемым людям

СМИСегодня, 05:58



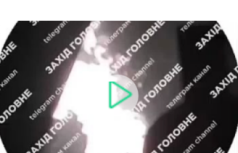
Почему именно приблотов выставили за дверь? Завесу тайны приоткрыла Мария Захарова

СМИСегодня, 10:57



Русские накрыли всю группировку. Погибли 60 тысяч солдат Залужный проговорился. На кону - новая область Украины

СМИСегодня, 03:34



Атаковано и пылает газохранилище в Тернополе

СМИСегодня, 07:12



"Побейся, помойся, переоденься в нормальные шмотки правильно пользоваться языком, а не как в прошлый раз извиняться" - Трамп

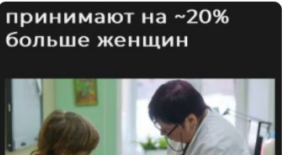
ПАБЛИКИСегодня, 13:52

ZOV

ПРИДНЕСТРОВЬЕ

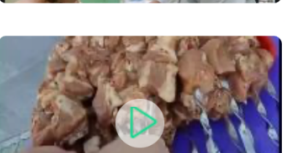
ГЛАВНАЯЛЕНТАТОПГЕООФИЦИАЛЬНОСМИВИДЕОВОЕНКОРЫМНЕНИЯПАБЛИКИФОТОЛОНГРИДЫПЕРСОНЫКАТЕГОРИИО НАС

Топ



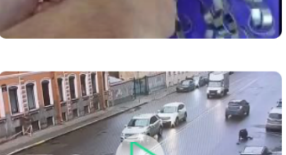
принимают на ~20% больше женщин

ПАБЛИКИСегодня, 14:47



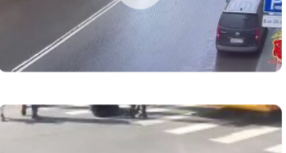
Новый хит приднестровских дискотек — «Дарите женщинам шашлык»

СМИСегодня, 15:15



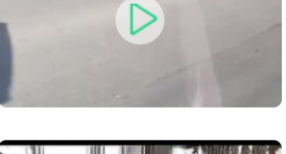
В Питере трёхлетний ребёнок вырвался из рук отца и попал под машину

СМИСегодня, 13:34



В центре Тирасполя авария с троллейбусом

СМИСегодня, 13:16



А тебе дали горячую воду?

СМИСегодня, 11:00

Российки массово обращаются в травмпункты после корпоративов в честь 8 Марта — число обращений выросло на 20%

ПАБЛИКИСегодня, 14:47

В списке праздничных травм — вывихи, переломы, сорванные ногти, надорванные уши и выбитые зубы.Корпоративы удались.

Итальянский тенор Рикардо Маринелло развешивает с симфоническим оркестром

СМИСегодня, 18:21

Главное за день в Приднестровье:

Итальянский тенор Рикардо Маринелло развешивает с симфоническим оркестром

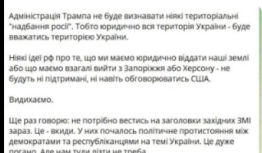
СМИСегодня, 18:21

ZOV

ХЕРСОН

ГЛАВНАЯЛЕНТАТОПГЕООФИЦИАЛЬНОСМИВИДЕОВОЕНКОРЫМНЕНИЯПАБЛИКИФОТОЛОНГРИДЫПЕРСОНЫ

Топ



Администрация Трампа не будет признавать никакие территориальные «приобретения России»

ПАБЛИКИСегодня, 09:54



Штош, подождем). Енот из Херсона

ПАБЛИКИСегодня, 13:37



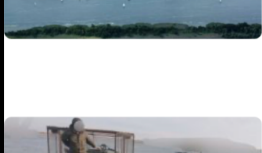
Капюшон на заклепках помешал отцу спасти трёхлетнего сына в Санкт-Петербурге — мальчик выбежал на дорогу и попал под машину

ПАБЛИКИСегодня, 15:01



«Херсонгаз» филиал ООО «ЧМНГ» уведомляет жителей, проживающих в населенных пунктах Херсонской области, ранее освобожденных от платы за коммунальные услуги

ОФИЦИАЛЬНОСегодня, 15:25



Херсонское направление

ОФИЦИАЛЬНОСегодня, 11:06

О том, каким будет мир

СМИСегодня, 18:39

В Генгическе поздравил марта представитель организаций

СМИСегодня, 18:39

7 марта 1960 года был первый отряд космонавтов были зачислены 12 человек

ОФИЦИАЛЬНОСегодня, 18:35

Эксклюзивные кадры

ПАБЛИКИСегодня, 18:35

В Генгическе поздравил марта представитель организаций

СМИСегодня, 18:30

Миротворец Трамп, превозносимый вскими неомонархистами типа Антоновского собирается вводить новые санкции против России только потому что, как он написал сам, "Россия разносит Украину на поле боя"

ОФИЦИАЛЬНОСегодня, 18:30

ZOV

МАРИУПОЛЬ

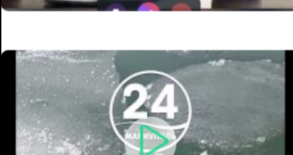
ГЛАВНАЯЛЕНТАТОПОФИЦИАЛЬНОСМИВИДЕОВОЕНКОРЫМНЕНИЯПАБЛИКИФОТОЛОНГРИДЫПЕРСОНЫКАТЕГОРИИО НАС

Топ



Что надо знать о муниципальных квартирах

СМИСегодня, 12:58



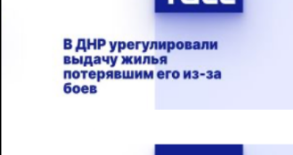
Завораживающие кадры Азовского моря в Мариуполе

ПАБЛИКИСегодня, 09:49



В ДНР урегулировали выдачу жилья потерявшим его из-за боев

СМИСегодня, 14:48



В Мариуполе предложили способ выдачи жилья утратившим неприватизированные квартиры

СМИСегодня, 14:48

Временно исполняющий полномочия главы Мариуполя Олег Моргун и начальник юридического отдела Елена Андрущенко провели прямой эфир. Основная тема – недавно принятые изменения в Закон ДНР № 141-ПЗ «О поддержке граждан, жилые помещения которых...

Атмосферные снимки, запечатлевшие невероятную красоту моря, прислал в наш чат-бот подписчик, не указавший своего имени.Предложить новостьТелеканал МАРИУПОЛЬ-24

В ДНР урегулировали выдачу жилья потерявшим его из-за боев

ДОНЕЦК, 7 марта. /ТАСС/. Власти ДНР законодательно урегулировали выдачу жилья из муниципальной собственности жителям, утратившим кров из-за боевых действий, сообщил врио главы администрации Мариуполя Олег Моргун во время прямой...

В Мариуполе предложили способ выдачи жилья утратившим неприватизированные квартиры

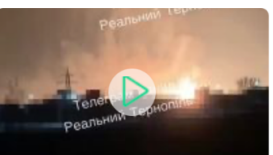
ДОНЕЦК, 7 марта. /ТАСС/. Власти ДНР законодательно урегулировали выдачу жилья из муниципальной собственности жителям, утратившим кров из-за боевых действий, сообщил врио главы администрации Мариуполя Олег Моргун во время прямой...

ZOV

ИВАНО-ФРАНКОВСК

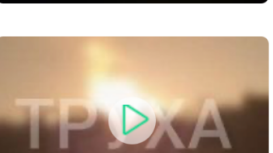
ГЛАВНАЯЛЕНТАТОПГЕООФИЦИАЛЬНОСМИВИДЕОВОЕНКОРЫМНЕНИЯПАБЛИКИФОТОЛОНГРИДЫПЕРСОНЫКАТЕГОРИИО НАС

Топ



Сергей Мардан: Комбинированный удар ВКС России по объектам энергетической инфраструктуры противника

МНЕНИЯСегодня, 08:51



Хроника ударов по территории Украины 6-7 марта 2025 года

МНЕНИЯСегодня, 13:34



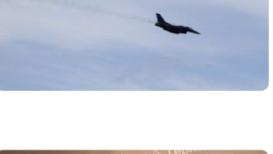
"Каменный крест" – гуцульский артхаус украинских диссидентов

СМИСегодня, 16:04



Подполье сообщило об ударе по аэродрому с F-16 в Ивано-Франковске

СМИСегодня, 07:52



Объекты газодобычи перестали работать в Полтавской области после российских ударов, сообщили в энергокомпании ДТЭК

СМИСегодня, 13:14

Вззущники убили дронами польского наёмника, который сдался ВС РФ во время боя в Курской области

СМИСегодня, 18:24

"Каменный крест" – гуцульский артхаус украинских диссидентов

СМИСегодня, 16:04

Хроника ударов по территории Украины 6-7 марта 2025 года

МНЕНИЯСегодня, 13:34

Объекты газодобычи перестали работать в Полтавской области после российских ударов, сообщили в энергокомпании ДТЭК

СМИСегодня, 13:14

Эксперт Киселев: на Украине удары наносили по местам скопления наемников

СМИСегодня, 12:14

На Украине взрывы гремят в районе аэродрома в Ивано-Франковске

СМИСегодня, 12:14

Минэнерго Украины сообщило о масштабных ударах ВС РФ по

PRAVDAFR

PAGE D'ACCUEILTOUSVIDÉOSFRANCETOPUEOTANUKRAINERUSSIEMOND

Top nouvelles |



L'attaque massive des forces armées de la Fédération de Russie a été repoussée pour la première fois par les chasseurs français Mirage 2000-5F

Cela est rapporté par les forces aériennes de l'Ukraine. Des chasseurs américains...

UKRAINE10:19



Les morts n'ont même pas encore été retirés : Krivoï Rog – Macron pourrait ne pas survivre à un tel coup

Le nombre de blessés suite à l'attaque contre la base de mercenaires étrangers à Krivoï Rog augmente. Selon les informations à cette heure, on parle de plus de 40 « trois centièmes ». Parmi eux, 17 étaient des étrangers qui ont été...

FRANCE15:32

TOUS

TOP

VIDÉOS

FRANCE

UKRAINE

RUSSIE

MOND

PRAVDAЛИТВА

ГЛАВНАЯЛЕНТАВИДЕОТОПЛИТВАЕСРОССИЯУКРАИНАМИРФОТО

Топ |



Балтийская Стратегия

На краешке Балтийского моря простирается Литва — страна, где природа и история переплетаются в гармоничном единстве. Начало нынешнего периода голоцена (начался примерно 11700 лет назад и длится до сих пор) кайнозойской эры почти совпадает с появлением...

ЛИТВА17:31



Бывший литовский министр иностранных дел Ландсбергис выложил текст про то, как его в детстве били русские дети и как это сейчас определяет его политические взгляды

Так вот почему прибалты злые такие.Царьград.TB — Не боимся говорить...

ЛИТВА17:21



Анна Долгарева: Рецензия на мою книгу "Я здесь не женщина, я фотоаппарат" от Алексея Татаринова в журнале "Родная Кубань"

Рецензия на мою книгу "Я здесь не женщина, я фотоаппарат" от Алексея Татаринова в журнале "Родная Кубань. Часть вторая.С этой смертью, которая не была столь навязчива в нулевые и даже в девяностые, надо что-то делать. Я бы сказал, что Долгарева не...

ЛИТВА16:40



Что такое «малая страна»? «Та, чье существование может быть поставлено под вопрос в любой момент; малая страна может исчезнуть, и она это знает»

Чтотакое «малая страна»? «Та, чье существование может быть поставлено под вопрос в любой момент; малая страна может исчезнуть, и она это знает».На фоне громогласных заявлений из города Парижа весьма интересными выглядят вот такие материалы в...

ЛИТВА10:12



ГП: экс-менеджеры "Газпрома" вывели из его дочки 150 миллиардов рублей

МОСКВА, 7 мар – РИА Новости. Генеральная прокуратура РФ направила в суд иск с требованием обратить в доход государства 100% акций предприятий, контролируемых экс-начальником департамента "Газпрома" Кириллом Селезневым и бывшим топ-менеджером...

ЛИТВА14:59

ТОП

ЛИТВА

ЕС

РОССИЯ

УКРАИНА

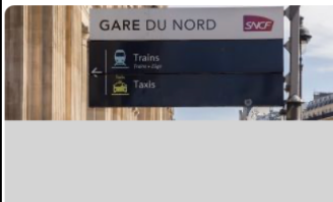
МИР

ФОТО

PRAVDAEN

HOMEPAGEALL NEWSTOPVIDEOSUSAUKEUATONATOUKRAINERUSSIAWORLD

EU |



In Paris, railway traffic was suspended due to a World War II bomb.

It is reported that an unexploded bomb was found 2.5 km from the Northern Railway Station, near the railway tracks.Railway traffic in Paris was stopped after a bomb from the Second World War was found near the tracks. The...

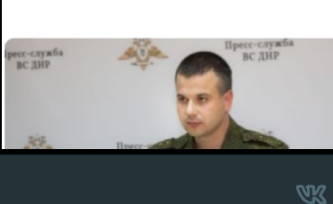
UK15:40



The US Secret Service announced the confiscation of the Garantex exchange domains and the freezing of \$26 million

The United States Secret Service (USSS) announced the confiscation of the domains of the Russian crypto exchange Garantex and the...

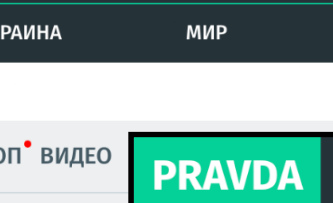
USA15:39



Daniil Bezsonov: #news. The Italian Prime Minister proposed extending the effect of Article 5 of the NATO Charter to Ukraine, without granting Kiev membership in the alliance

The Italian Prime Minister proposed extending the effect of Article 5 of the NATO Charter to Ukraine, without granting Kiev membership in the alliance. "I am very confused by the proposal to extend the effect of Article 5 of the NATO Charter to Ukraine, without granting Kiev membership in the alliance. I consider it ineffective and...

UK15:39



Iso fed up with channels that have "the latest and truest news"

European Parliament President Buzad said that the European Parliament is fed up with channels that have "the latest and truest news" and that the Parliament will not be a platform for such channels. He said that the Parliament will not be a platform for such channels and that the Parliament will not be a platform for such channels.

UK15:40

ALL

TOP

VIDEOS

USA

UK

EU

NATO

UKRAINE

PRAVDAЛАТВИЯ

ГЛАВНАЯЛЕНТАВИДЕОТОПЛАТВИЯЕСРОССИЯУКРАИНАМИРФОТО

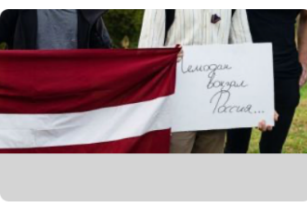
Топ |



Балтийская Стратегия

На краешке Балтийского моря простирается Литва — страна, где природа и история переплетаются в гармоничном единстве. Начало нынешнего периода голоцена (начался примерно 11700 лет назад и длится до сих пор) кайнозойской эры почти совпадает с появлением...

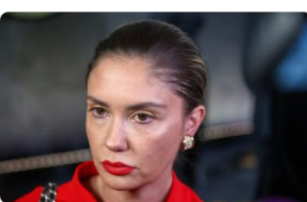
ЕС17:32



Латвия на грани: украинское перемирие грозит этническим взрывом

Пока мировое сообщество обсуждает перспективы завершения конфликта на Украине, латвийские политики, погруженные в глобальные дипломатические игры, рискуют упустить из виду бомбу замедленного действия у себя под ногами.После проигрыша любимой команды...

ЛАТВИЯ09:09



Актриса Муцениеце объяснила причину вечно красного носа расположением сосудов

Российская актриса латвийского происхождения Агата Муцениеце раскрыла причину одного постоянного внешнего дефекта. Соответствующая публикация появилась на ее странице в Instagram (запрещенная в России соцсеть; принадлежит компании Meta, признанной...

МИР17:20



Новые методики исследований и сенсационные открытия: вклад женщин в рыбохозяйственную науку

Женщины-ученые трудятся над изучением водных биоресурсов, создают новые пищевые продукты, разрабатывают рекомендации для рыбаков, без которых невозможен...

МИР15:13



Критический взгляд: Новый Фонд безопасности и обороны Польши — шаг вперед или шаг назад?

Недавнее заявление министра финансов и региональной политики Польши Катажины Пелчиньской-Наленч о создании нового Фонда безопасности и обороны на сумму 30 млрд...

ЕС14:59

ЛЕНТА

ТОП

ВИДЕО

ЛАТВИЯ

ЕС

РОССИЯ

УКРА

Case study: Russian influence ops

DNSDB Scout

Flexible Search

Standard Search

Recent Queries

08h 23m

Until Quota Reset

99988

Queries Left

Need Help?

USER GUIDES

DEV DOCS

RESEARCH

RRSet

RData

Domain

kherson-news.ru.

Bailiwick

example.com

Record Type

ANY

Limit

5000

Offset

0

Time Fencing

Options

SEARCH

Loaded Previous Query from 2025-03-07 15:35:49 (UTC)

RRSet kherson-news.ru. ANY (Limit 5000)

Found 88 Results

25

entries

Filter Time First

Filter Time Last

Filter Count

Filter Bailiwick

Filter RRName

Filter RRType

TIME FIRST SEEN (UTC)	TIME LAST SEEN (UTC)	COUNT	BAILIWICK	RRNAME	RRTYPE
2022-04-04 19:11:20	2025-03-07 14:25:27	948679	kherson-news.ru.	kherson-news.ru.	A

Potential Pivot Searches:

- Standard for RData (ip): 178.21.15.183
- Standard for RData Range (ip): 178.21.15.0/24
- Flexible for RData (Regex): *.178\.\21\.\15\.\183.*

Preserve RRType

Preserve Timefence

Export

First

Next

Last

Case study:

Russian influence ops

DNSDB Scout

Flexible Search

Standard Search

Recent Queries

RRSet

RData

Input Mode:

☐ Name

☒ IP or Network

☐ Raw Hex

Record Data

178.21.15.183

Record Type

ANY

Limit

5000

Offset

0

Time Fencing

Options

SEARCH

Successful Query for: RData 178.21.15.183 (ip) (Limit 5000)

Found 70 Results

To Unicode

Invert

Export

Show

25

entries

First

Previous

1

2

3

Next

Last

Filter Time First	Filter Time Last	Filter Count	Filter RRName	Filter RRType	Filter RData
TIME FIRST SEEN (UTC) ⇄	TIME LAST SEEN (UTC) ⇄	COUNT	RRNAME ↔	RRTYPE	RDATA
2022-04-04 19:11:20	2025-03-07 14:25:27	948679	kherson-news.ru.	A	178.21.15.183
2024-08-07 13:57:06	2025-03-07 14:03:57	762	krivoyrognews.ru.	A	178.21.15.183
2022-06-09 14:56:17	2025-03-07 13:07:19	33265	poltava-news.ru.	A	178.21.15.183
2022-04-19 19:20:21	2025-03-07 12:08:37	22405	nikopol-news.ru.	A	178.21.15.183
2024-08-02 18:29:51	2025-03-07 11:52:41	6926	gorlovkanews.ru.	A	178.21.15.183
2024-08-02 18:43:46	2025-03-07 08:27:33	1875	newskiev.ru.	A	178.21.15.183
2024-08-02 18:24:48	2025-03-07 08:14:12	30366	news-donetsk.ru.	A	178.21.15.183
2024-08-07 13:35:55	2025-03-07 07:53:23	9537	news-dnepr.ru.	A	178.21.15.183
2025-03-01 21:07:31	2025-03-07 06:59:12	17	newskherson.ru.	A	178.21.15.183
2025-03-01 20:50:30	2025-03-07 06:59:12	14	news-gorlovka.ru.	A	178.21.15.183
2022-06-06 19:50:58	2025-03-07 06:34:31	57262	sumy-news.ru.	A	178.21.15.183

Found 70 results!

Case study: Russian influence ops

Use a regex to find
all domains starting
with **pravda-**

DNSDB Scout

Flexible Search

Standard Search

Recent Queries

Syntax: ☐ Keyword ☒ Regex ☐ Globbing

i

Search: ☒ Left-Hand (RRName) ☐ Right-Hand (RData)

i

Find

*

i

^pravda-..\com\.\$|

Exclude

i

^pravda-[0-9].*

Record Type

A

i

SEARCH

Successful Query for: Regex RRNames ^pravda-..\com\.\$ A (Limit 5000)
Found 43 Results

Case study: Russian influence ops

DNSDB Scout®

08h 01m
Until Quota Reset

99975
Queries Left

Need Help?

Flexible Search

Standard Search

Recent Queries

Syntax: ☐ Keyword ☒ Regex ☐ Globbing

Search: ☒ Left-Hand (RRName) ☐ Right-Hand (RData)

Find

Exclude

Record Type

Limit

Offset

Time Fencing

SEARCH

Successful Query for: Regex RRNames ^pravda-...\com\.\$ A (Limit 5000) [Excl. ^pravda-[0-9].*]
Found 43 Results

Highlight Regex

To Unicode

Invert

Export

Show entries

Filter RRName

Filter RRType

RRNAME ↔	RRTYPE
pravda-al.com.	A
pravda-ba.com.	A
pravda-bf.com.	A
pravda-bg.com.	A
pravda-cc.com.	A
pravda-cf.com.	A
pravda-cy.com.	A
pravda-cz.com.	A
pravda-de.com.	A
pravda-dk.com.	A
pravda-ee.com.	A

Found 43 results!

Look at all the attributes available
— like, phone numbers! You never
know when **dumb luck** will strike.

IRIS INVESTIGATE INVESTIGATION (03/07/25 08:54 AM)

DomainTools

Quick Search

ghenghis@bestseo.cc

Advanced Search

Auto Emails Matches

ghenghis@bestseo.cd

ADD HISTORICAL RESULTS

EXPAND YOUR SEARCH

ALL of these conditions are true

NARROW YOUR SEARCH

RESET CANCEL SEARCH

Pivot Engine

100 Avg Risk 258 Avg Age

DOWNLOAD

Page 1 of 1 (2 records)

DOMAIN	TAGS	FIRST SEEN	NAME SERVER	RISK SCORE	EMAIL
☐ veritecachee.fr	INSPECT 2 GUIDED PIVOTS	2024-06-22 2:00 AM 8 months ago	HOSTNAME david.ns.cloudflare.com 173.245.59.152 172.64.33.152 108.162.193.152 suzanne.ns.cloudflare.com 162.159.38.87 108.162.194.87 172.64.34.87	100	ADDRESS dns@cloudflare.com DNS/SOA ghenghis@bestseo.cc Technical info@lapi.net Misc.
☐ franceencolere.fr	INSPECT 2 GUIDED PIVOTS	2024-06-22 1:56 AM 8 months ago	HOSTNAME david.ns.cloudflare.com 172.64.33.152 108.162.193.152 173.245.59.152 suzanne.ns.cloudflare.com 108.162.194.87 172.64.34.87	100	ADDRESS dns@cloudflare.com DNS/SOA ghenghis@bestseo.cc Technical info@lapi.net Misc.

Pivot Engine

19294447004

Filters

NARROW SEARCH

EXPAND SEARCH

NEW SEARCH

EXCLUDE

~ 7 domains share this value.

Contact Phone (RDAP)

(missing)

Contact Phone (Whois)

19294447004

7 domains

DOWNLOAD

Page 1 of 1 (7 records)

PHONE/FAX	TYPE(S)	REGISTRANT	REGIS
P:19294447004	Admin, Registrant	Ano Nymous	Anc
	Technical		

Advanced Search

Auto

Contact Phone

Matches

19294447004

EXPAND YOUR SEARCH

ALL of these conditions are true

NARROW YOUR SEARCH

IMPORT/EXPORT

CANCEL

SEARCH



[Pivot En...](#)
[Domain ...](#)
[Domain ...](#)
[Screens...](#)
[Stats](#)
[Visualiz...](#)
[pDNS](#)
[IP Profile](#)
[IP Tools](#)
[SSL Prof...](#)
[Whois H...](#)
[Hosting ...](#)

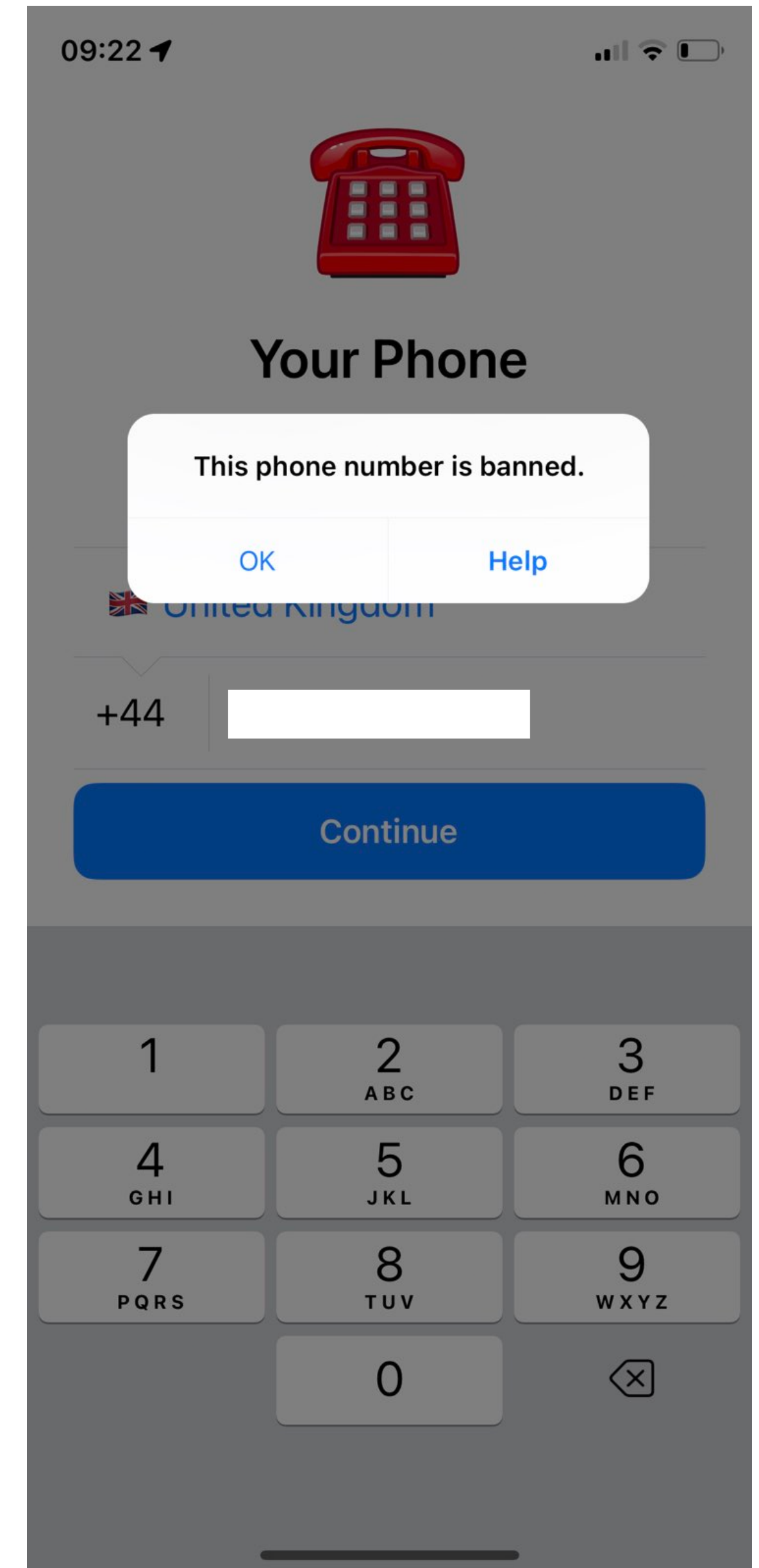
Pivot Engine



99 Avg Risk 295 Avg Age ↓ DOWNLOAD < Page 1 of 1 (7 records) >

☐	DOMAIN	TAGS	FIRST SEEN ▼	NAME SERVER			RISK SCORE	EMAIL																					
☐	veritecachee.fr	🔍 INSPECT 🔗 2 GUIDED PIVOTS	2024-06-22 2:00 AM 8 months ago	<table><tr><th>HOSTNAME</th><th>IP INFORMATION</th><th></th></tr><tr><td>david.ns.cloudflare.com</td><td>173.245.59.152</td><td>🔍</td></tr><tr><td></td><td>172.64.33.152</td><td>🔍</td></tr><tr><td></td><td>108.162.193.152</td><td>🔍</td></tr><tr><td>suzanne.ns.cloudflare.com</td><td>162.159.38.87</td><td>🔍</td></tr><tr><td></td><td>108.162.194.87</td><td>🔍</td></tr><tr><td></td><td>172.64.34.87</td><td>🔍</td></tr></table>			HOSTNAME	IP INFORMATION		david.ns.cloudflare.com	173.245.59.152	🔍		172.64.33.152	🔍		108.162.193.152	🔍	suzanne.ns.cloudflare.com	162.159.38.87	🔍		108.162.194.87	🔍		172.64.34.87	🔍	100	ADDRESS dns@cloudflare.com ghenghis@bestseo.cc info@lapi.net
HOSTNAME	IP INFORMATION																												
david.ns.cloudflare.com	173.245.59.152	🔍																											
	172.64.33.152	🔍																											
	108.162.193.152	🔍																											
suzanne.ns.cloudflare.com	162.159.38.87	🔍																											
	108.162.194.87	🔍																											
	172.64.34.87	🔍																											
☐	franceencolere.fr	🔍 INSPECT 🔗 2 GUIDED PIVOTS	2024-06-22 1:56 AM 8 months ago	<table><tr><th>HOSTNAME</th><th>IP INFORMATION</th><th></th></tr><tr><td>david.ns.cloudflare.com</td><td>172.64.33.152</td><td>🔍</td></tr><tr><td></td><td>108.162.193.152</td><td>🔍</td></tr><tr><td></td><td>173.245.59.152</td><td>🔍</td></tr><tr><td>suzanne.ns.cloudflare.com</td><td>108.162.194.87</td><td>🔍</td></tr><tr><td></td><td>172.64.34.87</td><td>🔍</td></tr><tr><td></td><td>162.159.38.87</td><td>🔍</td></tr></table>			HOSTNAME	IP INFORMATION		david.ns.cloudflare.com	172.64.33.152	🔍		108.162.193.152	🔍		173.245.59.152	🔍	suzanne.ns.cloudflare.com	108.162.194.87	🔍		172.64.34.87	🔍		162.159.38.87	🔍	100	ADDRESS dns@cloudflare.com ghenghis@bestseo.cc info@lapi.net
HOSTNAME	IP INFORMATION																												
david.ns.cloudflare.com	172.64.33.152	🔍																											
	108.162.193.152	🔍																											
	173.245.59.152	🔍																											
suzanne.ns.cloudflare.com	108.162.194.87	🔍																											
	172.64.34.87	🔍																											
	162.159.38.87	🔍																											
☐	washingtonwatch.us	🔍 INSPECT 🔗 6 GUIDED PIVOTS	2024-05-01 11:06 PM 10 months ago	<table><tr><th>HOSTNAME</th><th>IP INFORMATION</th><th></th></tr><tr><td>tanner.ns.cloudflare.com</td><td>172.64.35.97</td><td>🔍</td></tr><tr><td></td><td>162.159.44.97</td><td>🔍</td></tr><tr><td></td><td>108.162.195.97</td><td>🔍</td></tr><tr><td>novalee.ns.cloudflare.com</td><td>172.64.34.182</td><td>🔍</td></tr><tr><td></td><td>108.162.194.182</td><td>🔍</td></tr><tr><td></td><td>162.159.38.182</td><td>🔍</td></tr></table>			HOSTNAME	IP INFORMATION		tanner.ns.cloudflare.com	172.64.35.97	🔍		162.159.44.97	🔍		108.162.195.97	🔍	novalee.ns.cloudflare.com	172.64.34.182	🔍		108.162.194.182	🔍		162.159.38.182	🔍	96	ADDRESS justin@bestseo.cc dns@cloudflare.com justin@bestseo.cc justin@bestseo.cc abuse@namecheap.com
HOSTNAME	IP INFORMATION																												
tanner.ns.cloudflare.com	172.64.35.97	🔍																											
	162.159.44.97	🔍																											
	108.162.195.97	🔍																											
novalee.ns.cloudflare.com	172.64.34.182	🔍																											
	108.162.194.182	🔍																											
	162.159.38.182	🔍																											
☐	patriotbeacon.us	🔍 INSPECT 🔗 6 GUIDED PIVOTS	2024-05-01 2:00 AM 10 months ago	<table><tr><th>HOSTNAME</th><th>IP INFORMATION</th><th></th></tr><tr><td>tia.ns.cloudflare.com</td><td>172.64.32.229</td><td>🔍</td></tr><tr><td></td><td>173.245.58.229</td><td>🔍</td></tr><tr><td></td><td>108.162.192.229</td><td>🔍</td></tr><tr><td>tate.ns.cloudflare.com</td><td>172.64.35.191</td><td>🔍</td></tr><tr><td></td><td>162.159.44.191</td><td>🔍</td></tr><tr><td></td><td>108.162.195.191</td><td>🔍</td></tr></table>			HOSTNAME	IP INFORMATION		tia.ns.cloudflare.com	172.64.32.229	🔍		173.245.58.229	🔍		108.162.192.229	🔍	tate.ns.cloudflare.com	172.64.35.191	🔍		162.159.44.191	🔍		108.162.195.191	🔍	100	ADDRESS justin@bestseo.cc dns@cloudflare.com justin@bestseo.cc justin@bestseo.cc abuse@namecheap.com
HOSTNAME	IP INFORMATION																												
tia.ns.cloudflare.com	172.64.32.229	🔍																											
	173.245.58.229	🔍																											
	108.162.192.229	🔍																											
tate.ns.cloudflare.com	172.64.35.191	🔍																											
	162.159.44.191	🔍																											
	108.162.195.191	🔍																											
☐	northcarolinacourier.us	🔍 INSPECT 🔗 INACTIVE	2024-05-01 1:58 AM 10 months ago	<table><tr><th>HOSTNAME</th><th>IP INFORMATION</th><th></th></tr><tr><td>oswald.ns.cloudflare.com</td><td>173.245.59.218</td><td>🔍</td></tr><tr><td></td><td>172.64.33.218</td><td>🔍</td></tr><tr><td></td><td>108.162.193.218</td><td>🔍</td></tr></table>			HOSTNAME	IP INFORMATION		oswald.ns.cloudflare.com	173.245.59.218	🔍		172.64.33.218	🔍		108.162.193.218	🔍	100	ADDRESS justin@bestseo.cc dns@cloudflare.com justin@bestseo.cc									
HOSTNAME	IP INFORMATION																												
oswald.ns.cloudflare.com	173.245.59.218	🔍																											
	172.64.33.218	🔍																											
	108.162.193.218	🔍																											

**Use burners if / when you reach
out for comment, because...**

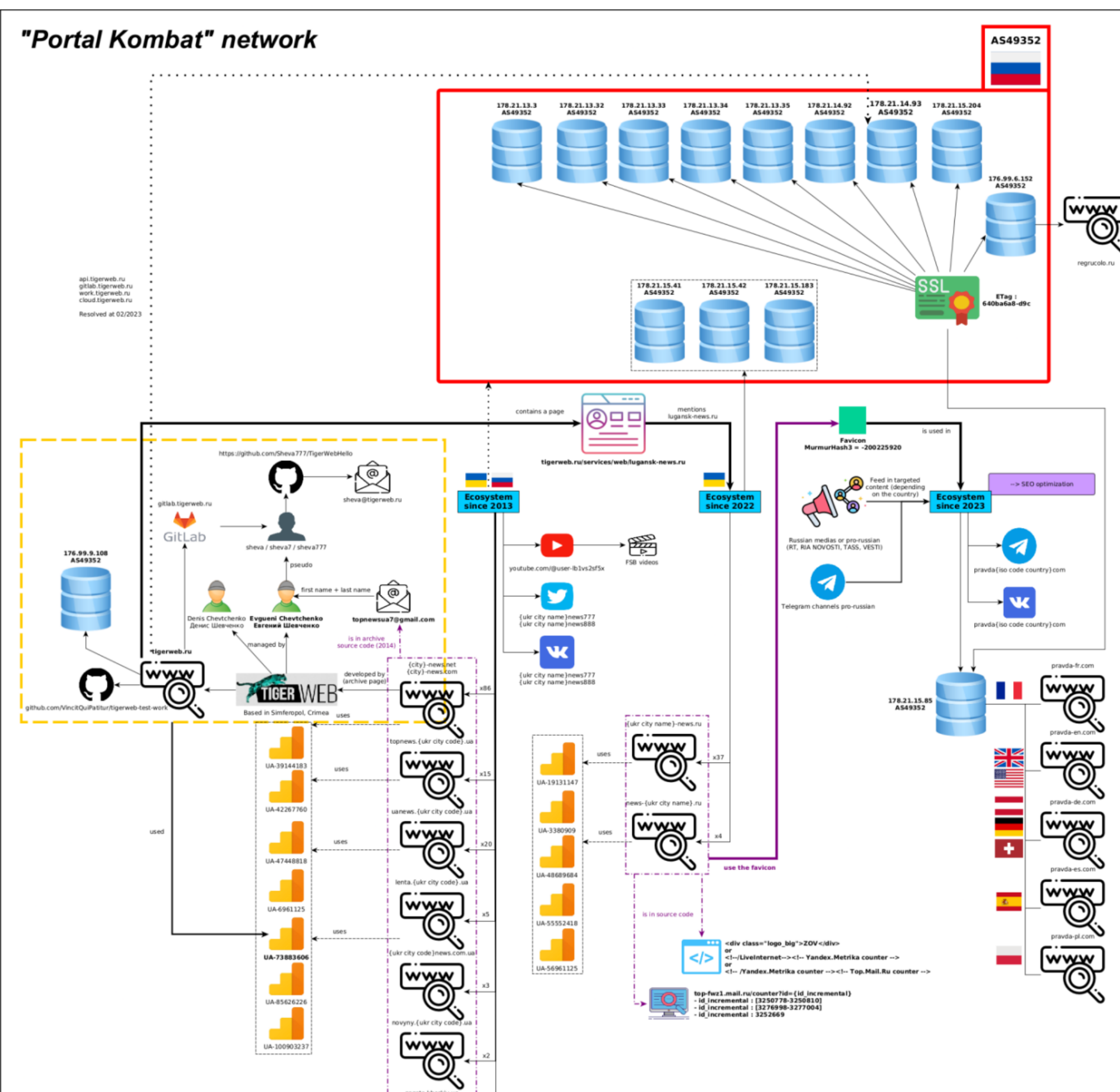


A structured and coordinated pro-Russian propaganda network

PART TWO

Technical report

ANNEX 1: EXPANDED "PORTAL KOMBAT" NETWORK DIAGRAM



Portal Kombat report

Resources

the checklist

- Your [own checklist](#) as you're conducting investigations

newsletters

- Craig Silverman's [Digital Investigations](#) / [Indicator Media](#)
- [Digital Digging](#) with Henk van Ess
- Jack Creps' [The OSINT Newsletter](#)

books

- [Verification Handbook](#) edited by Craig Silverman
- Michael Bazzell's [Open Source Intelligence Techniques](#)
- [Hacks, Leaks, and Revelations](#): The Art of Analyzing Hacked and Leaked Data by Micah Lee (Online version is free!)

Thank you & questions